Mayank V. Bendarkar, Darshan Sarojini, Evan Harrison, Dimitri N. Mavris. "Evaluation of Off-Nominal Performance and Reliability of a Distributed Electric Propulsion Aircraft during Early Design", AIAA Scitech 2021 Forum (AIAA 2021-1723)
https://doi.org/10.2514/6.2021-1723 , https://arc.aiaa.org/doi/10.2514/6.2021-1723

Evaluation of Off-Nominal Performance and Reliability of a Distributed Electric Propulsion Aircraft during Early Design

Mayank V. Bendarkar*, Darshan Sarojini†, Evan Harrison‡, and Dimitri N. Mavris§
Aerospace Systems Design Laboratory, School of Aerospace Engineering
Georgia Institute of Technology, Atlanta, Georgia, 30332

General Aviation (GA) is likely to be at the forefront of a paradigm change in aviation, where the introduction of novel concepts such as Urban Air Mobility (UAM), architectures like $e-$VTOL, and technologies like Distributed Electric Propulsion (DEP) are expected to make aircraft more efficient and reduce their environmental footprint. However, these architectures carry with them an uncertainty related to the off-nominal operational risk they pose. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new technologies. While a lot of the literature surveyed focuses on improving traditional methods of safety analysis, it still does not completely address the limitations caused due to insufficient knowledge and experience with transformative technologies. The research objective of the present work is to integrate the Bayesian safety assessment framework developed previously by the authors with conceptual and 6-DoF performance models for DEP aircraft to evaluate off-nominal performance and reliability using information that is typically available in conceptual or preliminary design phases. A case study on the electric power architecture of the the NASA *Maxwell* X-57 Mod. IV is provided. A maximum potential flight path angle metric, as well as trimmability considerations using a 6-DoF model constructed using available literature help determine hazard severity of power degradation scenarios. Bayesian failure rate posteriors are constructed for the different components in the traction power system, which are used in a Bayesian decision framework. The results indicate that while most of the components in the traction power architecture of the X-57 Mod. IV are compliant with failure rate requirements generated, the batteries, cruise motors, and cruise motor-inverters do not meet those requirements.

Nomenclature

V_∞	=	Free-stream velocity
h	=	Altitude
γ	=	Flight path angle (climb)
θ	=	Pitch angle
ϕ	=	Bank angle
ψ	=	Yaw angle
δ_e	=	Elevator deflection
δ_a	=	Aileron deflection
δ_r	=	Rudder deflection
τ_L	=	Left wingtip engine throttle (fraction of max power)
τ_R	=	Right wingtip engine throttle (fraction of max power)
HLP	=	High Lift Propulsors

*Senior Graduate Researcher, ASDL, School of Aerospace Engineering, Georgia Tech, AIAA Student Member
†Senior Graduate Researcher, ASDL, School of Aerospace Engineering, Georgia Tech, AIAA Student Member
‡Research Engineer II, ASDL, School of Aerospace Engineering, Georgia Tech, AIAA Member
§S.P. Langley Distinguished Regents Professor and Director of ASDL, Georgia Tech, AIAA Fellow

I. Introduction

General Aviation (GA) is likely to be at the forefront of a paradigm change in aviation, where the introduction of novel concepts such as Urban Air Mobility (UAM), architectures like $e-$VTOL, and technologies like Distributed Electric Propulsion (DEP) are expected to make aircraft more efficient and reduce their environmental footprint. However, these architectures carry with them an uncertainty related to the off-nominal operational risk they pose. To ensure the continued safety of the GA fleet and operations in this rapidly evolving new paradigm, the Federal Aviation Administration (FAA) implemented a new set of performance-based certification rules for Normal Category Aircraft in Title 14 of the Code of Federal Regulations (CFR), Part 23, Amendment 64 [1]. Of particular interest in this work is 14 CFR §23.2510 which requires that all equipment, systems, and installations have [1]

"a logical and acceptable inverse relationship between the average probability and the severity of failure conditions."

It is paramount for aircraft designers to have the capability to quantify safety risk earlier in the design phases to help mitigate avoidable surprises once the aircraft is already built. The simplest definition of safety risk in literature generally involves quantifying it as a combination of two entities – the probability of a failure or an unsafe event, and the severity associated with it [2]. The intent of safety assessments is to ensure that any system under consideration poses no worse than an acceptable level of risk, with Table 1 showing allowable probability requirements for different failure condition classifications. SAE ARP4754 and SAE ARP4761 are considered as accepted and well established guides for performing safety assessments [2, 3], with Figure 1 giving the integration of system safety with the traditional systems engineering V. It shows that safety and reliability requirements in aircraft design are allocated to the item or component level following a hierarchical decomposition of aircraft functions and architecture. Safety requirements are initially functionally decomposed at the aircraft level, followed by a *flow-down* of the aircraft level functions to generate the system level requirements. The analyses conducted at these levels include both aircraft and system level Functional Hazard Analysis (FHA), Common Cause Analysis (CCA), and a Preliminary System Safety Assessment (PSSA). In terms of the aircraft design timeline, these correlate well with the conceptual and preliminary design phases. As the design matures, Fault Tree Analysis (FTA) is conducted at aircraft and system level. As the aircraft is built, these analyses and the requirements generated are verified, thus travelling back up the 'V'. While this work focuses on incorporating safety analysis earlier in the design of novel system concepts, a comprehensive coverage of traditional safety assessment tools is not considered here. Interested readers are directed to literature for a more comprehensive coverage of the traditional safety assessment tools and methods [2, 4–8]. Similarly, readers interested in understanding the processes, requirements, and management of artifacts for certification are directed to articles from a parallel effort that looks at incorporating a Model-Based Systems Engineering (MBSE) approach to certification by the authors [9, 10].

To summarize, the current paradigm seeks to identify hazards early in the design process and percolate corresponding qualitative or quantitative safety requirements downstream. Washington et al.[11] summarize the outcome of the system safety assessment process as four related sets F, C, Λ and O where:

1) F is the set of n identified failure conditions $f_1 \; - \; f_n$
2) C is the set of severities c_i assigned to each failure condition f_i
3) Λ is the set of probabilities λ_i of each failure condition f_i, and
4) O is the set of failure probability objective o_i associated with f_i and its severity c_i as given by table 1

Table 1 Quantitative Allowable Failure Rate for Different Failure Conditions [12]

Assessment Level	Failure Condition Classification				
	Negligible	Minor	Major	Hazardous	Catastrophic
I	No Probability Requirement	$<10^{-3}$	$<10^{-4}$	$<10^{-5}$	$<10^{-6}$
II		$<10^{-3}$	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$
III		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-8}$
IV		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$

The current safety assessment paradigm is not without its limitations. In the conceptual and preliminary design phase, the existing approach of safety assessment seeks to limit the risk posed by any failure condition f_i by ensuring that the probability of said failure λ_i is less than its probability objective o_i as determined by Table 1 using severity c_i. Novel architectures and technologies like a distributed electric propulsion (DEP) aircraft may not have discrete functional failures, and their consequences may not be well understood. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new technologies. This

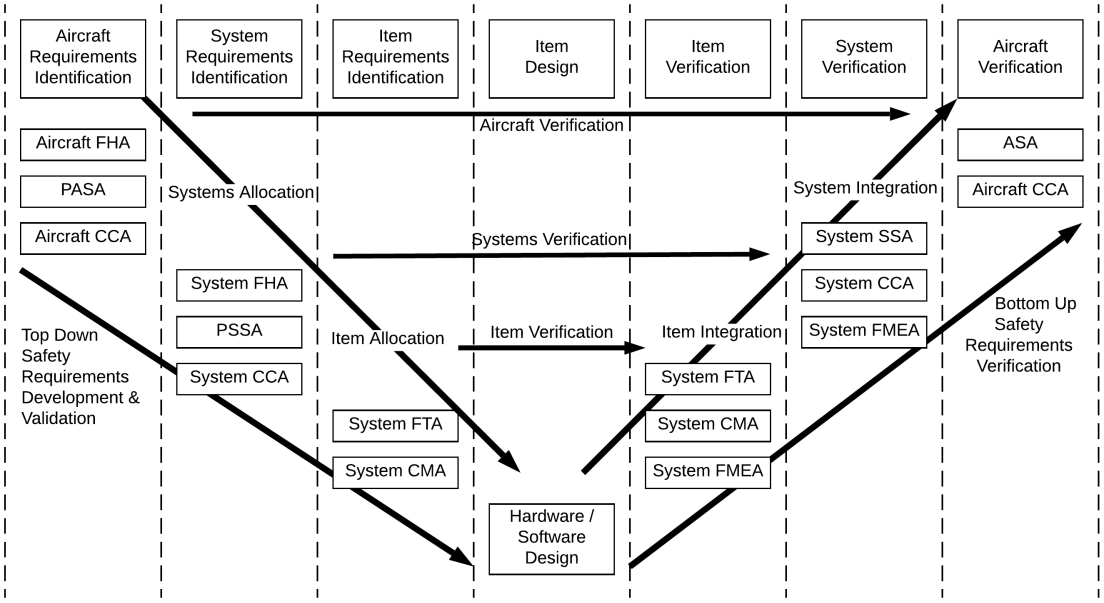


Fig. 1 The System V & V diagram in the context of safety and aircraft design (Adapted from ARP4754 [3])

can considerably affect the adoption of new technologies since the knowledge required to certify these products is unavailable due to the lack of operational experience. One solution in the traditional approach is to assign a conservative estimate to the severity posed, resulting in incorrect unit level probability requirements (o_i) in the early design process. As Armstrong states in his PhD thesis [13]:

> "Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements."

The research objective of the present work is to demonstrate the utility of the Bayesian safety assessment framework developed by Bendarkar et al. [14] on a Distributed Electric Propulsion (DEP) concept – NASA's *Maxwell* X-57 Mod-IV. Preliminary and 6-DoF performance and flight simulation models have been created for the same to evaluate its off-nominal performance and safety risk using information that is typically available in conceptual or preliminary design phases. The rest of this paper is organized as follows: Sec. II provides some background and literature pertaining safety analysis techniques and their applicability to the X-57, Sec. III summarizes the implemented Bayesian framework to evaluate off-nominal performance and safety using dynamic performance models, Sec. IV provides a step by step case study of implementing the proposed framework on the X-57 Mod. IV using some conceptual level metrics and then trim solutions using a preliminary 6-degree-of-freedom (DoF) model followed by conclusions (Sec V). Appendix B provides additional details on the environment used to create the 6-DoF model as well as other details that do not form the focus of the present work but are useful for interested readers.

II. Background and Literature

Before we can discuss traditional and state-of-the-art methods to perform risk analysis, we must answer the questions: i) "What is risk?", and ii) "What makes it acceptable?". Risk and its estimation, typically involves providing answers to the following three questions: i) what can go wrong?, ii) how likely is it?, and iii) what is the consequence? In one of the seminal works on quantitatively defining risk, Kaplan and Garrick suggest a *'set of triplets'* idea – where risk is denoted by a triplet of i) scenario, ii) likelihood, and iii) consequence, to answer the three questions given above [15]. In determining what constitutes an "acceptable risk", they pose two difficulties with the problem itself – one minor and one major. The 'Minor' difficulty is that risk is not linearly comparable – two different risks cannot always simply be compared*. The 'Major' difficulty, which also serves as the answer to this underlying question, is that risk cannot be considered in isolation, but only in combination with the costs and benefits of the alternatives attendant to it. Thus, once we decide to fly, we must accept some inherent risk, with a baseline given by the risk posed by concepts and technologies

*e.g. consider the famous Trolley problem [16–18] and the risks posed to the persons on the tracks

available to us today. It is with this understanding that we proceed with the task of estimating and comparing (to make a decision on compliance) the risks posed by novel aircraft concepts and architectures. For the discussion that follows, we revert to a *'hazard severity & probability'* paradigm to assess risk and make it comparable. A hazard is typically considered as a *'source of danger'*, which combined with the likelihood of precipitating it into damage or loss, gives us the risk [15].

A lot of research has gone into improving traditional methods of risk analysis – methods like Hazard and Operability Study (HAZOP) [19] and extensions to Faults Trees [20] are popular. However, both of these maintain the limitations of the traditional methods when it comes to assessing novel aircraft like the X-57. Model Based Dependability Analysis (MBDA) explores how dependability information (hazard severity) can be synthesized from system models automatically, and shows promise in evaluating novel technologies [21]. Safety and reliability considerations while designing an aircraft electrical systems have been of interest for a long time [22]. Hasan et al. [23] and Hemm et al. [24] utilized modeling and simulation tools to gain additional knowledge regarding hazard severity and probabilities while focusing on the operational safety paradigm. Papathakis et al. [25] and Woodham et al. [26] conducted safety assessments of novel electric propulsion technologies. However in all these, variants of traditional methods like FTA and FHA have been utilized with subject matter expert knowledge to conduct safety assessments of novel aircraft technologies. They still do not completely address the problem of insufficiency of knowledge and experience with transformative technologies, and therefore share the same limitations mentioned in Sec. I.

Thus, determining hazard severity remains one of the biggest problems with determining safety risk and reliability of novel aircraft concepts and architectures, especially since there is little historical data or precedent to inform the analyst. In such a situation, an approach that utilizes system performance and dynamic models seems to show promise. Dynamic probabilistic risk analysis (DPRA) was originally developed to evaluate nuclear reactor safety [27]. While failure dynamics in the nuclear industry play out over long periods of time, in aircraft, the system transient period post failure is a few seconds long, with two components failing in quick succession extremely improbable. Thus, stochastic transitions due to failures can be modeled independently of the system dynamics [28]. Dominguez-Garcia et al. [28] proposed a methodology that uses a behavioral model for system performance and dynamics with artifacts to model component failure, along with Markov chains for modeling the different configurations (states) a system can adopt under component failures to enable dynamic performance and reliability evaluation of fault-tolerant systems. In a case study on a lateral-directional flight control system of a fighter aircraft, they demonstrated that using a quantitative system behavioral model allowed the assessment of the "*degree of failure*" along with degraded system operational modes [28]. In another study that utilizes system models to determine the effects of component failure on critical functions, Borer et al. [29] evaluated two critical portions of proposed NASA Lunar Surface Systems. When physical components were mapped to system critical functions, a direct simulation of component dependencies (power, thermal etc.) resulted in identification of cascading failures and allowed determination of architectural features that drive system loss probability [29]. Thus, surveyed literature suggests that multi-state reliability assessment methods that utilize system performance and behavioral models show promise while determining hazard severity for novel aircraft concepts and architectures. While prior work has looked at utilizing exclusively dynamic models, the present work will focus on system performance models at the conceptual stage (static) as well as preliminary 6-DoF models (dynamic) to characterize the response of the system to component level failures.

The literature discussed so far focuses on methods to accurately determine hazard severity, but there is another problem with utilizing traditional approaches to characterize safety of novel configurations. Traditional methods to compute probability, given in ARP 4761 cannot comprehensively address uncertainty in input data and models [11]. Uncertainty is of two primary types [30] – $aleatory$ uncertainty refers to inherent randomness in the system, while $epistemic$ uncertainty refers to uncertainty due to lack of knowledge. For novel aircraft concepts and architectures, the aleatory uncertainty is large due to lack of available data, while the limited knowledge and experience available for these aircraft results in a large epistemic uncertainty as well. A work-around for this seems to come in the form of methods like parametric Weibull analysis that try to capture uncertainty better [31, 32]. This requires knowledge about the detailed working of every component and may not be best suited for early design phases when such information is not available.

The next section seeks to address the above mentioned shortfalls by presenting the safety analysis framework utilized for the present work. It intends to augment traditional safety assessment methods by allowing model-based estimation of hazard severity and a Bayesian approach to probability of failures for novel concepts and technologies.

III. A Bayesian Safety Framework utilizing System Performance Models

The safety analysis framework discussed in this section was introduced in prior work by Bendarkar et al. [14], and will be summarized here for completeness.

A. Severity Assessment & Reliability Requirement Allocation

1. Extension of Continuous Functional Hazard Analysis (C-FHA)

The functional decomposition of a novel system architecture or technology is likely to remain similar to a conventional system even if the implementation varies drastically between the two. Traditional Functional Hazard Assessment (FHA) utilizes this knowledge to keep implementation and behavioral spaces independent while characterizing hazards [33]. Traditional FHA considers discrete off-nominal scenarios, for e.g. – 1)loss of function, 2) excess function, and 3)incorrect operation of function. However, for novel concepts and architectures like a distributed electric propulsion (DEP) aircraft, one may have continuous range of functional degradation scenarios. As a result, it is important to differentiate off-nominal scenarios that can result in continuous functional degradation (e.g. losing two out of 12 DEP propulsors), as against the traditional discrete loss scenarios (e.g. one engine out). Continuous-FHA extends the traditional FHA and system safety analysis methods to consider the magnitude of function loss when assessing an architecture or a concept [33]. Additionally, a concept like DEP may have stronger interdependence between different functions that are not found in traditional concepts. For instance, loss of thrust for a DEP can entail losing propulsors in different locations, which in turn can have a strong impact on lateral equilibrium.

Figure 2a provides a notional plot showing how hazard severity can be obtained as a function of continuous functional degradation. The effect of functional degradation is computed on various safety metrics using available models for a particular flight phase. Decision makers can then utilize this knowledge to define hazard severity curves for every case, which can then be combined into one hazard severity curve for the function under consideration for the flight phase of interest. This final hazard severity - function loss curve now provides a physics backed relationship between the two, as opposed to a heuristic and case by case approach provided by traditional FHA. The continuous hazard severity results in safety requirements that are allocated to the system level functions in terms of allowable failure rate (see Table 1).

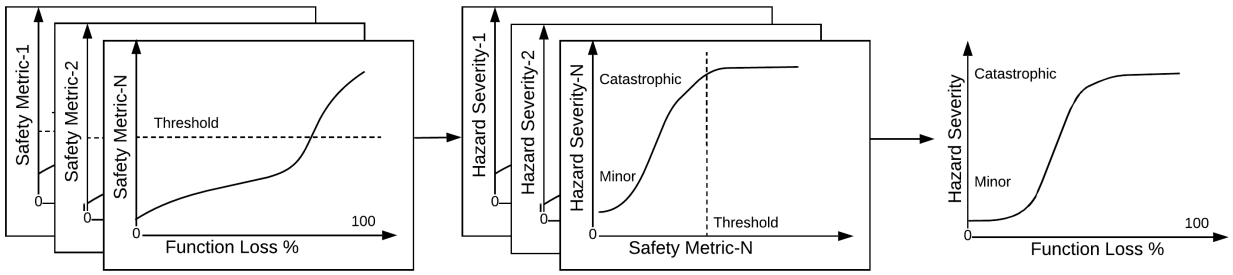
Failures in source or intermediate components are likely to result in degradation in the system's capability to perform certain functions. A system model that can quantify the effect of component failure on the system level functions can now be utilized to generate component level reliability requirements based on generated hazard severity-functional degradation relationship. As shown notionally in Fig. 2b, if the failure of component A or B results in a 50% and 25% functional degradation at the system level, the requirement for allowable failure rates for these components can be generated by utilizing the inverse relationship between hazard severity and probability requirement.

2. A Network Approach to Bottom-Up Failure Analysis

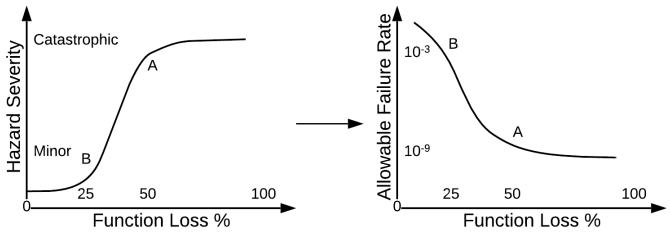
The next step involves conducting a bottom-up failure analysis to determine the system level impact of component-level failures. Allocation of failure rate (reliability) requirements to the component level can be achieved if component failures can be characterized in terms of degradation of system level functions, since the relationship between hazard severity and functional degradation is already established (see Fig. 2a).

If we consider a system as a network (directed acyclic graph) of components required to satisfy a function, an adjacency matrix can be created to represent it mathematically. The reliability of such a network can then be found using techniques available in literature [34]. Figure 3 shows a notional, partially redundant architecture of components connecting a prime-mover A_B (typically energy storing or power generating component) to a terminal consumer A_T that performs the system level function, along with its network representation as an adjacency matrix. In such situations, network reliability concepts can be utilized to automatically determine the effect of failures in the prime-movers A_B as well as intermediate components $A_{1\to6}$ on the terminal function providers A_T. This is enabled through the algorithm given in the Appendix C.

For a DEP architecture, A_T may represent one of many propulsors that provide thrust, while A_B may represent a power source like a battery. The failure of a single component may result in multiple propulsors failing – in such a situation, a set of all of failures that result in unique system level effects must be constructed. Utilizing a network approach thus facilitates the automated determination of the impact of component failures on system level functional degradation, lending well to the proposed methodology.



(a) Hazard severity with continuous functional degradation



(b) Allowable failure rate for the given severity curve

Fig. 2 Notional plot of the C-FHA process [14]

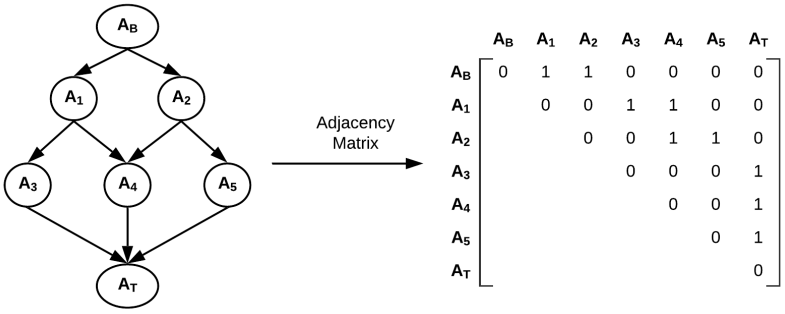


Fig. 3 Example network representation of component connectivity within a system architecture along with its adjacency matrix

B. Bayesian Probability Assessment

There are two schools of thought when it comes to defining probability - the *'frequentist'* (objective) and the *'Bayesian'* (subjective). A Bayesian approach of estimating probability allows for the treatment of both epistemic and aleatory uncertainty even when available data is limited. Kaplan and Garrick argue that when faced with insufficient data, there is no choice but to use a Bayesian approach [15]. Instead of only using data, a Bayesian approach relies on using information - which includes data, models, and other available information like subject matter expert (SME) knowledge [35]. Furthermore, a Bayesian inference model can be continuously updated as additional information becomes available. Bayesian inference techniques for safety and reliability assessment have been applied to numerous problems in literature [36–39] and are considered mature and mathematically sound for the purpose. The utility of this approach can be attested to when one considers that numerous industries consider these techniques standard [40–43].

Instead of a point estimate as under the *frequentist* paradigm, the failure rate (λ) in Bayesian probability theory is given by a distribution that quantifies uncertainty in its estimate. When available failure data ($\bar{y}$) is provided, the failure rate λ conditioned over $\bar{y}$ is given by the conditional distribution as given by Eq. 1.

$$p(\lambda|\bar{y}) = \frac{p(\bar{y}|\lambda)p(\lambda)}{p(\bar{y})} \tag{1}$$

Equation 1 gives the Bayesian posterior distritbution $p(\lambda|\bar{y})$ based on the likelihood of observing the data that was

observed $p(\bar{y}|\lambda)$ and the analyst's prior belief $p(\lambda)$, normalized over all realizations of the data $p(\bar{y})$. Note that Eq. 1 is simply a statement of Bayes' theorem applied to multiple independent identically distributed observations $\bar{y} = y_1, y_2, ...y_n$.

The likelihood $p(\bar{y}|\lambda)$ is a function that seeks to determine the likelihood of observing the data $\bar{y}$ given a value for λ. It is a statistical model used to represent the aleatory uncertainty associated with the data and the underlying physical phenomenon [11]. In the context of aircraft design, while numerous distributions can be used to model component failure data, the three most common distributions used are the Binomial, Poisson, and Exponential [35].

The prior distribution $p(\lambda)$ captures information that is denoted by the analyst's subjective state of belief regarding the failure rate. Since this distribution is based on the analyst's knowledge about the component or event, it captures the epistemic uncertainty associated with estimating the failure rate (λ) [11].

The posterior distribution provides an updated state of knowledge of the failure rate taking into account the analyst's subjective state of belief and available data. Certain heritage data can also be utilized by eliciting its applicability from subject matter experts (SMEs), and averaging the posterior distributions according to the applicability of the data [35]. When there is no data available, the posterior ends up being the same as the prior. The prior's influence on the posterior reduces as more and more data becomes available, resulting in the posterior moving closer towards the Frequentist estimate – thus a Bayesian framework naturally lends itself to a *'frequentist'* estimation as sufficient data becomes available. A Bayesian approach has numerous benefits over the traditional Frequentist approach (in addition to treating uncertainty more comprehensively) for application to safety assessment of novel aircraft concepts.

- The Bayesian posterior can be continuously updated as more data becomes available – the existing posterior is treated as a prior for the new data and a new posterior is generated.
- A 95% posterior credible interval for λ has a 95% probability of the true value of λ lying within it [44], unlike the more complicated interpretation of Frequentist confidence intervals[†]. This little fact enables us to create a decision theoretic framework as given in the following subsection.

C. Integrated Risk Assessment & Decision Framework

At this point, assuming the hypothetical components A and B from the C-FHA example in Fig. 2b have been allocated failure rate requirements after the end of the extended C-FHA process, it is also assumed that component failure probability posterior have been computed using the Bayesian approach explained above. Placing the probability requirements from extended C-FHA on the CDFs of the Bayesian failure posteriors, analysts can compute the probability with which reliability requirements can be met. This is shown notionally in Fig. 4.

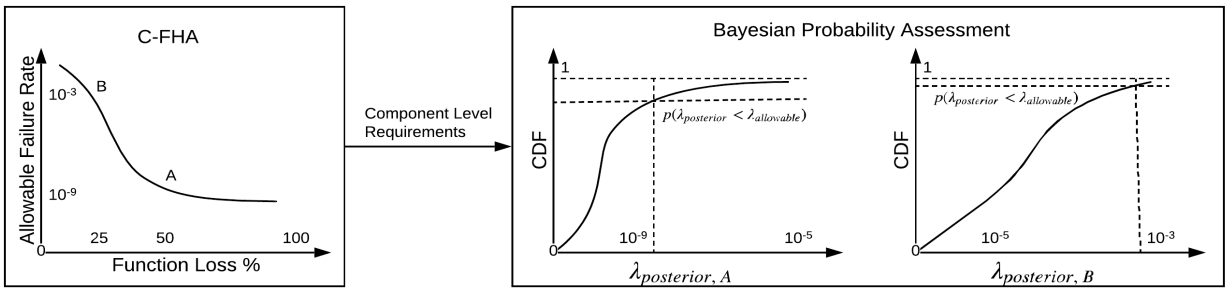


Fig. 4 Notional Integrated Risk Assessment - Probability of meeting component failure rate requirements [14]

Decision makers now need to make a decision on whether the corresponding probability of meeting requirement is good enough to consider component B compliant with the safety requirements. In a Bayesian decision theoretic setup, such a compliance decision regarding component B is considered an action a

$$a \in A,\ A = \{compliant, non-compliant\}$$

If the true value of the compliance finding (in reality - unknown) is given by x

$$x \in X,\ X = \{compliant, non-compliant\}$$

[†]A 95% Frequentist confidence interval states that if a sample of failure data were collected a large number of times, 95% of the generated confidence intervals will contain the true λ [44]; an interpretation that is not very useful in the current application.

then a loss function $L(x, a)$ can be defined to represent the penalty to be paid if the analyst chooses action a when the true compliance value is x, under available information $p(\lambda_{posterior} < \lambda_{allowable})$. In such a framework, the Bayesian expected loss $\rho(a, p)$ is the expectation of this loss function $L(x, a)$ with respect to the posterior failure rate, and is given by Eq. 2.

$$\rho(a, p) = \int_{\lambda} L(x, a) p(\lambda|\bar{y}) \delta\lambda \tag{2}$$

An action $a*$ that minimizes the expected loss given by Eq. 2 should be the action taken by the analyst, and is also called *Bayes action*. The integrated framework for evaluating compliance is shown in Figure 5. It is assumed in Fig. 5 that the configuration has been sized – this includes the weight breakdown including mass properties, geometric definitions including wing and other areas including locations of control surfaces if any, architecture definition that includes any redundancy considerations for the internal energy flows of the systems, any available aerodynamics and propulsion models, and finally any available subsystem sizing details. Adequate performance models to characterize the effect of functional degradation on safety metrics of interest are developed. These include models that can characterize the dynamic performance of the aircraft under off-nominal operations for different flight phases – take-off, climb, cruise, and landing. These models, that also allow the evaluation of component failures on system performance are utilized the complete the hazard severity assessment. Combined with the decision framework, a compliance finding of the novel architecture can be made.

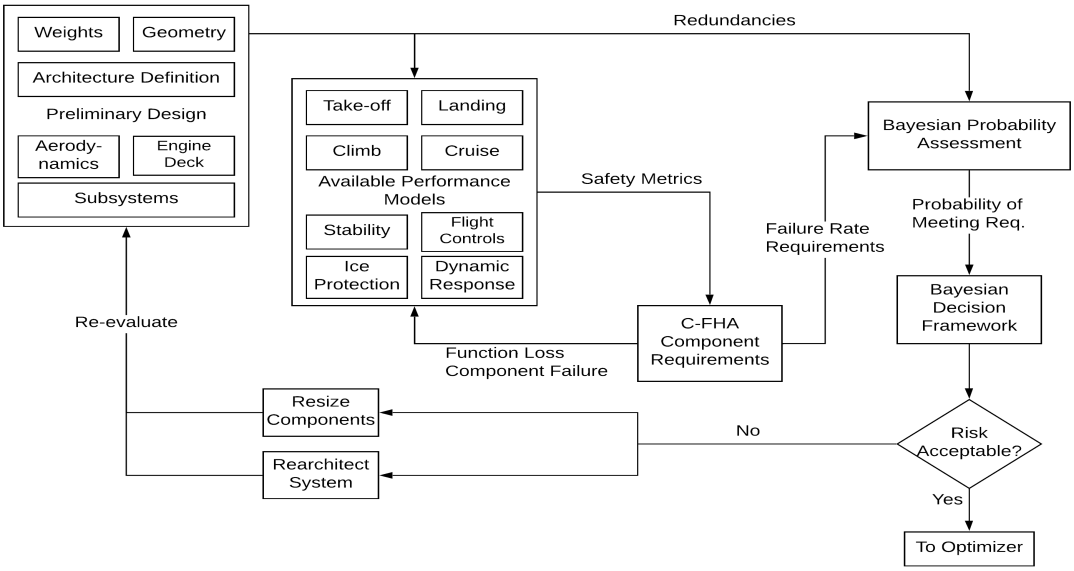


Fig. 5 Proposed framework for safety assessment integrated with design of novel architectures [14]

IV. Case Study: The X-57 Aircraft

A novel configuration- the X-57 is chosen as a test-case aircraft to demonstrate the proposed method. The X-57 *Maxwell* is an experimental aircraft designed to demonstrate a 3.5 times aero-propulsive efficiency gain at a "high-speed cruise" flight condition for comparable general aviation aircraft by effectively utilizing propulsive airframe integration (PAI), made practical due to the progress made in electric propulsive powertrains [45]. To build the X-57, a Tecnam P2006T airframe is to be modified with a higher aspect ratio wing, with two main propulsive electric motors installed at the wingtips to power the cruise propellers. Another 12 electric motors in nacelle-pylons will power the high lift propellers distributed across the wing leading edge. This Distributed Electric Propulsion (DEP) architecture is expected to provide a higher dynamic pressure during takeoff and landing, while providing more efficient aero-propulsive performance during cruise. Overall, the X-57 is expected to achieve a five times lower energy use than the Tecnam P2006T [46]. Open-source data is available for this aircraft, making it a good candidate for studies.

In addition to the novel technologies being tested with the X-57 program, of interest in the present work are the tools and methods used to conduct safety analysis of such transformational aviation concepts. Research in this direction

available in literature points towards the utilization of traditional methods to assess safety [25, 26, 45]. Having multiple propulsors, the effect of one or more propulsors failing must be considered to assess the safety of the aircraft. Assessing the safety of the power system architecture of the X-57 will be the focus of the present work. To define and assess the safety metrics to be utilized in this exercise, a simple point-mass energy-based performance model is utilized. A 6-DoF simulator is then utilized for more detailed trimmability studies under off-nominal scenarios. The simulator, as well as the open-source data used to create the aircraft model is given in the Appendices A, B.

A. The X-57 Power System Architecture and Extended C-FHA

The X-57 Mod. IV reliability and off-nominal performance determined in the present case study will focus on its power system architecture adapted from Clarke et al. [45]. Figure 6 shows the X-57 power system network having two main batteries, traction buses, pre-chargers, and inverters supplying 30 kW each (half of required cruise power) to the wing-tip cruise motors. Similarly, each battery bus supplies three high lift motors on either side of the wing, providing good redundancy. The X-57 traction power system has been designed using a combination of available standards and best practices, since the traditional 14 CFR Part 23 and Part 25 provide little applicable guidance for electric power systems [45]. Clarke et al. [45] also performed a traditional safety analysis (FMECA[‡]) on this system, including all permutations of cruise or high lift motors failing. Since multiple failure modes of any component has the same effect at the system level, only single-point top level failure modes of the components were considered. Their results show two primary critical failure scenarios – (i) asymmetric thrust due to cruise motor failure, and (ii) in-flight battery fire. While the former results in untrimmable yawing moment using the stock rudder, the latter can result in total power loss and catastrophic structural failure. Both of these are potentially unrecoverable for the pilot. Additionally, Ref. [45] provides a failure scenario matrix providing criticality of single component failures. These results will therefore be utilized to benchmark the performance of the severity assessment method presented in the current work.

The function that is considered for severity analysis in the C-FHA method proposed in Sec. III is *'Generate Thrust'*, which in this case, is closely related to the function *'Generate Power'*. A functional degradation scenario is postulated next, and its effect on system level performance metrics quantified. The computation of appropriate safety metrics to evaluate the effect of functional degradation is vital to the success of the extended C-FHA process. One particular metric - the maximum potential climb gradient is discussed next.

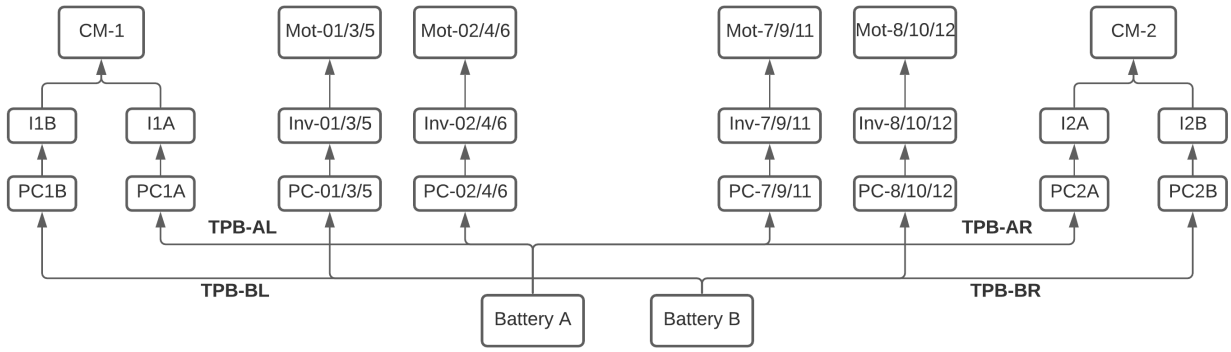


Fig. 6 The X-57 Mod IV power system representative diagram (Adapted from Ref. [45])

1. Specific Excess Power and Maximum Potential Climb Gradient

The specific excess power is a widely used, energy-based metric that allows aircraft conceptual designers to gauge an aircraft's performance (at zero bank angle) with respect to power available to climb (change in potential energy), or to accelerate (change in kinetic energy).

$$P_S = \frac{(T_{max} - D)\, V_\infty}{W} = \frac{d}{dt}\left(h + \frac{V_\infty^2}{2g}\right) \tag{3}$$

When the acceleration is zero, the specific excess power can go towards achieving the maximum potential flight path

[‡]Failure Modes, Effects, and Criticality Analysis

angle, which is given by:

$$\gamma_{max} = \arcsin(\frac{\frac{dh}{dt}}{V_\infty}) = \arcsin(\frac{P_S}{V_\infty}) \tag{4}$$

While looking at the criticality of off-nominal scenarios for the X-57's power system architecture in conceptual design, one can consider scenarios where thrust is degraded due to the loss of power to one (or multiple) cruise or distributed propulsors. These can be modeled as a reduction in maximum available thrust in Eq. 3. The thrust available at a particular altitude and velocity can be computed using Eq. 25 as well as the contribution from active distributed propulsors (see Tab. 15) provided in the appendix. The total aircraft drag is computed using Eq. 27 and Eq. 35, with a simplified polynomial fit generated given in Eq. 5 with coefficients as provided in table 2.

$$C_D = C_{D_0} + KC_L^2 + k_1 C_L \tag{5}$$

Table 2 Polynomial drag coefficients for different flap and high-lift propeller settings

	Flaps Retracted		Flaps Takeoff	
	HLP OFF	**HLP ON**	**HLP OFF**	**HLP ON**
C_{D_0}	0.0465	0.1878	0.1692	0.3047
K	0.0569	0.0433	0.0487	0.0393
k_1	-0.0414	-0.0596	-0.105	-0.107

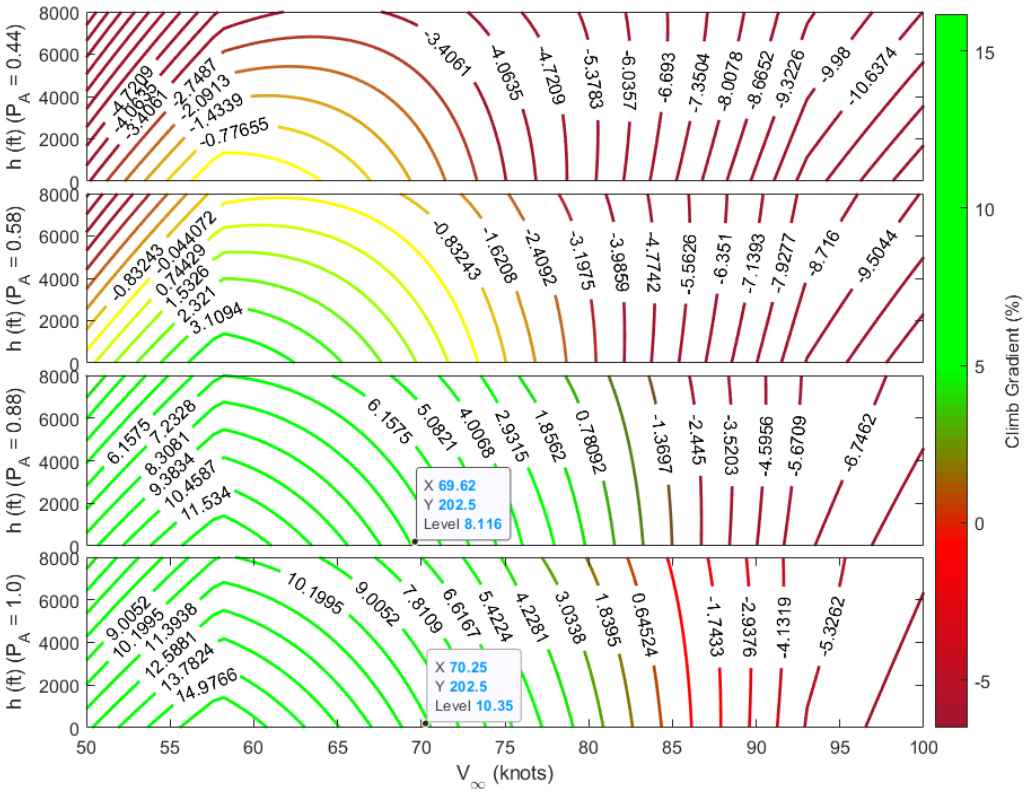


Fig. 7 Climb gradients at 44%, 58%, 88%, and 100% power available in take-off configuration with HLP *On*

The following discussion will focus on figures 7, 8 to determine the hazard severity (see table 1) for different power degradation scenarios. Figure 7 shows the maximum potential climb gradient (in %, $tan(\gamma_{max}) * 100$) for four different

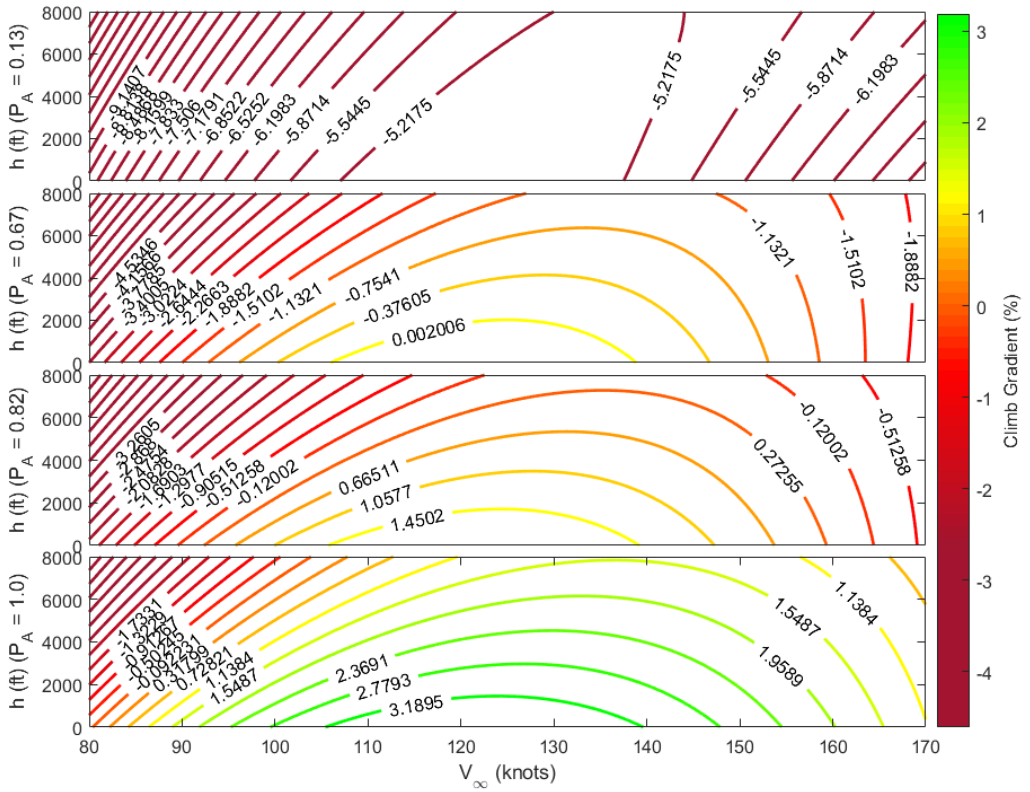


Fig. 8 Climb gradients at 13%, 67%, 82%, and 100% power available in cruise configuration

cases of power (or thrust) degradation. To begin, when there is no degradation in power available, the X-57 far exceeds the 8.3% climb gradient requirement posed by 14 CFR §23.2120(a)(1) at takeoff. While this requirement does not apply to a loss of thrust scenario, it can be seen that at a degradation in power of more than 12% ($P_A \leq 0.88$), the aircraft can no longer maintain a climb gradient of 8.3%. We can utilize this knowledge to assign a hazard severity of *'Major'* to a power loss of more than 12%.

Additionally, 14 CFR §23.2120(b)(1) requires the aircraft achieve a climb gradient of 1.5% at 5000 feet under a critical loss of thrust. It was found that under take-off configuration (flaps extended, high lift propulsors *On*), the X-57 can attain this value when faced with a 42% degradation in power available ($P_A = 0.58$). Any greater loss of thrust means that the aircraft cannot achieve the 1.5% climb gradient stipulated. While not dangerous by itself, this failure to meet regulatory requirements is given a higher than normal severity rating of *'Hazardous'* in the traditional hazard severity scale.

While defining traditional critical engine inoperative (CEI) scenarios may be challenging for novel concepts like the X-57, this demonstrates that a critical loss of thrust may be defined by utilizing performance metrics like climb gradients, and as will be discussed later, trimmability considerations. Conversely, the criticality of loss of power scenarios for DEP aircraft can be estimated in conceptual design using the same performance metrics. For instance, at $P_A = 0.44$ and below (power degradation of 56% or more), the aircraft can no longer achieve a positive climb gradient at sea level. Therefore, the hazard severity for this condition is classified as *'Catastrophic'*.

Results of similar analysis conducted for the cruise configuration (flaps retracted, HLP *Off*) are shown in figure 8. At nominal conditions ($P_A = 1$), the model predicts the X-57 to have reasonable climb performance all the way to cruise altitude (8000 ft). Note that the maximum potential climb gradient also corresponds to the most optimum flight condition ($(L/D)_{max}$). Quick computation provides cruise $(L/D)_{max} = 16.24$, which is close to values found in literature, at a velocity of approximately 137 knots.

Under off-nominal scenarios, a power (or thrust) degradation of 18% or more results in the aircraft being incapable of maintaining level flight at cruise altitude (visible in $P_A = 0.82$ contours). Since the aircraft has to descend to maintain steady level flight at a lower altitude, this condition is assigned a severity of *'Major'*.

A power (or thrust) degradation of more than 33% results in the aircraft being incapable of maintaining level flight at any altitude above sea-level ($P_A = 0.67$ contours). Since the aircraft is expected to be at well above 1500 feet (cruise configuration), this condition provides the pilots sufficient time to respond and glide the aircraft to (relative) safety. However, the pilots are left with no choice but to conduct an emergency landing, or to decelerate, descend, and activate the high lift propellers to enable steady level flight. This condition is therefore assigned a severity of *'Hazardous'*.

A traditional one engine inoperative (OEI) scenario is particularly interesting for the X-57. Excess power analysis suggests that the aircraft is forced to enter a descent of less than 3° glideslope. However, this case presents an interesting caveat in terms of trimmability that will be tackled in Sec. IV.A.3.

Finally, Fig. 8 shows that for a power degradation of 87% or more, the X-57 cannot maintain a descent gradient under -5.2% (−3°) at any combination of altitude and velocity. While the X-57 mission profile location has been restricted over Rogers dry lakebed (Edwards, California) to allow for a wide-range of landing options [45], this condition is categorized in the present work as *'Catastrophic'* for the reason that it endangers the one and only X-57 aircraft that will be produced. This failure also potentially applies to other future DEP aircraft which may face a similar limitation.

Table 3 summarizes the results discussed thus far. It demonstrates how hazard severity can be allocated as a function of continuous power degradation using the C-FHA method discussed in Sec. III.A.1. It is important to recognize that the X-57's maximum thrust available is different in the takeoff and cruise configurations due to the excess thrust provided by the high lift propellers. Therefore, the two configurations' C-FHA severity values need to be considered separately. The next part of this work will demonstrate how a network reliability approach can be utilized to determine the effect of component failures on the system level function, and help assign reliability requirements to the component level as is notionally suggested in Fig. 2b.

Table 3 Summary of continuous power degradation hazard severity based on the γ_{max} safety metric

Severity / **Configuration**	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Takeoff	$0.88 \leq P_A \leq 1$	$0.58 \leq P_A \leq 0.88$	$0.44 \leq P_A \leq 0.58$	$P_A \leq 0.44$
Cruise	$0.82 \leq P_A \leq 1$	$0.67 \leq P_A \leq 0.82$	$0.13 \leq P_A \leq 0.67$	$P_A \leq 0.13$

2. Utilizing the proposed Network Approach to a Bottom-up Failure Analysis

The components of interest in the X-57 traction power system, and their connectivity are given in Fig. 6. These include two batteries A and B and two traction power buses from each battery – TPB-AL, TPB-BL on the left, TPB-AR, TPB-BR on the right. These TPBs supply power to pre-chargers (PC) of three high lift motors each, and supply half the cruise requirements of the main cruise motor to the corresponding pre-chargers. The PCs control the initial power on current supplied to the inverters while behaving as a closed circuit after reaching steady state. The inverters supply power and control the different high lift and cruise motors. Each cruise motor thus receives half power from each battery, while three high lift motors on each side are supplied by the same battery, providing symmetric redundancy.

In terms of the notation in Sec. III.A.2, the batteries are the prime movers A_B, the electric motors are the terminal nodes A_T since they help fulfil the system level function of generating thrust, while all other components are intermediate components that facilitate the connection between the two. The generated adjacency matrix was processed using the algorithms given in the Appendix C to auto-generate a list component failures that result in different system level failure states (in terms of one or multiple electric motors failing to receive power). Since the effect of component failures on terminal components that satisfy system level functional requirements can be determined in an automated fashion, component failures can be placed on the C-FHA hazard severity plots. Hazard severity is then assigned to every component. Looking at the results, although the γ_{max} safety metric does not consider a cruise motor failure as critical during the takeoff phase, it is considered hazardous in the cruise configuration. A summary result of this process is given in table 4.

Only single component failures are explored in the present work since the probability of multiple components failing at once is considered negligible under independent failure assumption. Note that due to symmetry of the power systems architecture, only six distinct system level consequences are evaluated for component failure scenarios, with all other scenarios assumed identical to ones given in table 4. For instance, cruise motor-2 and CM-1 failures can be considered identical, Mot-01 failure is identical to any other high lift motor failing (except slight changes in yawing moments

generated), and effects of traction bus or battery failure is symmetrically identical to other buses or battery failure as well. While only the γ_{max} energy metric is utilized here to demonstrate the proposed safety method, other safety metrics are likely to provide different results. Interested readers are directed to work by Puranik [47, 48] for a list of other energy based metrics that can be considered as relevant for this effort. Finally, while allocating reliability requirements to the components, it is essential that the most critical hazard severity be utilized for a given component's failure.

The proposed extended C-FHA process for determining hazard severity may be stopped here during the early preliminary design stage to allocate reliability requirements to system components. If additional information/ knowledge about the design is available, this process may be extended to utilize higher fidelity models that incorporate system dynamics to determine the effect of failures on system level functions. In the next section, such an exercise is attempted. A 6-DoF model of the X-57 is generated to determine the trim solutions of the aircraft under off-nominal scenarios. A full dynamic analysis is omitted in the present work due to space constraints, and will be reported in a future publication.

Table 4 X-57 power architecture unique system level failure states and severity using the γ_{max} metric

Failed Component (causal factors)	System level failure states (Power loss to electric motors)	Proportion of maximum power available after failure (P_A for takeoff/cruise)	Hazard Severity (γ_{max} metric)
CM-1	CM-1	$P_{A_{TO}} = 0.84$, $P_{A_{cruise}} = 0.5$	Hazardous
PC-1B or Inv-1B	CM-1 at 50%	$P_{A_{TO}} = 0.92$, $P_{A_{cruise}} = 0.75$	Major
PC-01 or Inv-01 or Mot-01	Mot-01	$P_{A_{TO}} = 0.94$, $P_{A_{cruise}} = 1$	Minor
TPB-BL	Mot-1,3,5 ; CM-1 at 50%	$P_{A_{TO}} = 0.75$, $P_{A_{cruise}} = 0.75$	Major
Battery-B	Mot-1,3,5,8,10,12; CM-1,2 at 50%	$P_{A_{TO}} = 0.5$, $P_{A_{cruise}} = 0.5$	Hazardous
Battery-B (fire)	Mot-[1-12]; CM-1,2	$P_{A_{TO}} = 0.0$, $P_{A_{cruise}} = 0.0$	Catastrophic

3. Trimmability considerations using a Preliminary 6-DoF Model

The present work leverages the DELPHI framework developed at the Aerospace Systems Design Lab as the primary simulation environment. A preliminary 6-DoF model of the X-57 was developed inside DELPHI by using open source data available from various sources. Details regarding the framework (Appendix A) and the development of the X-57 model (Appendix B) are provided in the appendix for interested readers. DELPHI allows the explicit definition of each individual high lift propulsor, along with its thrust, drag, moments, and mass properties applied first to its individual local axis, and transformed to the aircraft axis (Appendix B..1, B..2, B..3). The aerodynamic properties and stability/control derivatives are extracted from openly available data where applicable, or generated using a vortex lattice method otherwise (Appendix B..4). Overall, the generated model allows simulating the aircraft for any permutation of high lift propulsors and/or cruise motors active, for any permutations of aircraft states and environmental conditions. At its heart, the model computes the total forces and moments generated by each explicitly defined cruise / high lift propellers and any aerodynamic surfaces about the CG of the aircraft. Finally a trim algorithm proposed by Marco et al. [49] that utilizes a minimization technique to determine a trim solution for any input combination of aircraft state, control deflections, environmental conditions, and propulsive state is utilized with the 6-DoF model. The trim objective is to match the mission V_∞, h, while maintaining wings level ($\phi = 0$) and maximizing γ.

Table 5 shows the results of trim analysis on different failure states. The bank angle (ϕ) was forced to remain zero for all of these solutions, except one as indicated in the configuration column. Three different mission segments were considered in particular based on mission profiles suggested by Schnulo et al. [50, 51] (with some exceptions) – i) Takeoff configuration (HLP On, Flaps 30°) at 50 feet and $1.2V_{S1}$ or 69.6 knots, ii) HLP On, Flaps 0° at 1500 feet and 83.5 knots, and iii) Cruise configuration at 1500 feet and 105 knots.

Under a failure scenario where the left cruise motor cannot provide any thrust, the aircraft can still attain approximately a 3% climb gradient with almost maximum rudder deflection. However, if the failure occurs at 1500 feet with the aircraft at 83.5 knots, no trim solutions were found with the climb gradient greater than −5.6% and maximum rudder deflection. This condition therefore drives the reliability requirement for the cruise motor by assigning a severity of *'Hazardous'* to its failure. It is interesting to note that while conceptual studies suggest that the rudder has enough control authority to maintain the second cruise motor at maximum of 50% thrust in a cruise motor our scenario, present results indicate that the aircraft is trimmable with a 87% throttle setting on the right motor in the cruise configuration at 105 knots and a descent gradient of approximately −3%

Table 5 X-57 unique system level failure states and severity using trim solutions

Failed Component	Failure State	Mission Segment			Aircraft States			Flight Controls					Severity
		Configuration	V_∞ (knots)	h (ft)	$\tan(\gamma_{max})$ (%)	θ (deg)	ψ (deg)	δ_e (deg)	δ_a (deg)	δ_r (deg)	τ_L	τ_R	
CM-1	CM-1	Takeoff	69.6	50	2.97	2.89	-2.48	-3	1	-15.6	0	0.57	Hazardous
		HLP ON Flaps 0	83.5	1500	-5.6	-0.32	-2.37	-5	1.26	-15.7	0	0.70	
		Cruise	105	1500	-2.97	4.9	-2.00	-5	13.74	-15.0	0	0.87	
PC-1B Inv-1B	CM-1 at 50%	Takeoff	69.6	50	6.03	4.6	-2.52	-3	1	-15.81	0.5	0.76	Major
		HLP ON Flaps 0	83.5	1500	-2.37	1.74	-2.42	-5.16	1.3	-16	0.5	0.85	
		Cruise	105	1500	-1.22	5.88	-1.48	-5	1.28	-11.13	0.5	0.9	
PC-01 Inv-01 Mot-01	Mot-01	Takeoff	69.6	50	9.98	7.34	-0.94	-3.06	0.4	-5.96	0.9	0.9	Minor
		HLP ON Flaps 0	83.5	1500	1.17	4.4	-0.25	-5.33	0.15	-1.69	0.9	0.9	
TPB-BL	Mot-1,3,5, CM-1 at 50%	Takeoff	69.6	50	1.4	3.07	-2.5	-2.97	1.18	-16.0	0.5	0.58	Hazardous
		HLP ON Flaps 0	83.5	1500	-3.5	3.2	-2.36	-5.68	1.57	-15.77	0.5	0.79	
		Cruise	105	1500	-1.05	5.97	-1.56	-5.0	1.35	-15.45	0.5	0.90	
		Takeoff (ϕ = 2.73°)	74	5000	1.5	4.92	5	-3.5	2.2	-12.67	0.5	0.88	(regulatory)
Battery-B	Mot-1,3,5, 8,10,12, CM-1,2 at 50%	Takeoff	69.6	50	-1.17	4.48	0	-3.35	0	0	0.5	0.5	Catastrophic
		HLP ON Flaps 0	83.5	1500	-6.3	4.1	0	-6.35	0	0	0.5	0.5	
		Cruise	105	1500	-4.54	4	0	-5	0	0	0.49	0.49	
Battery Fire	Mot-[1:12], CM-1,2	Takeoff	69.6	50	-9.3	4.56	0	-6	0	0	0	0	Catastrophic
		HLP OFF Flaps 30	83.5	1500	-7.98	-0.91	0	-3.82	0	0	0	0	
		Cruise	105	1500	-7.34	2.43	0	-5	0	0	0	0	

A slightly less severe failure is when either of prechargers or inverters supplying the cruise motors fail. In such a situation, the aircraft maintains 50% power (thrust) from one cruise motor while the other is free to operate at any power setting. The X-57 can maintain a climb gradient of over 6% just after takeoff in this situation, but has to make an emergency landing if this occurs during any other mission segment. Therefore, this condition is assigned a severity of *'Major'*.

When one of the distributed propulsors lose power (near the wingtip is more critical than near the fuselage), the aircraft can continue to climb after takeoff with little effect on its performance. At 83.5 knots and 1500 feet though, the climb gradient was found to be rather limited. This was found to be more a limitation of the high lift propeller thrust dropping with velocity, than an effect of the failure. Lower velocities were found to improve the climb performance at 1500 feet. Thus, a severity of *'Minor'* feels justified for this situation.

Losing one of the four traction power buses (B-Left in this instance) was found to have a severity of *'Major'* in the conceptual stage (see Sec. IV.A.1). However, under a trim analysis, this failure is found to afford a maximum trimmable climb gradient of just 1.4% at takeoff. Additionally, if this failure occurs at higher velocities, the aircraft can be forced to descent or to dump excess kinetic energy to attain steady level flight. The conceptual analysis given in Sec. IV.A.1 suggested the critical loss of thrust (14 CFR §23.2120(b)(1)) to be defined at a power degradation scenario of 42%. However, as can be seen in table 5, the aircraft is barely trimmable with a loss of traction power bus (25% power degradation) with almost maximum rudder deflection as well as a non-zero bank angle. No trim solutions were found for this condition with $\phi = 0°$. Due to the preceding arguments, this condition is assigned a severity of *'Hazardous'*.

Finally, while conceptual level analysis (see Sec. IV.A.1) determined that the aircraft could takeoff and climb with a battery failure, trim analysis could find no solution for the aircraft to do so in any of the evaluated mission segments. In fact, if a battery fails right after takeoff, the aircraft was found to trim with a maximum climb gradient of -1.7%. Therefore, the severity of this failure state is escalated to *'Catastrophic'*.

A battery fire was already considered catastrophic by Ref. [45] and from Sec. IV.A.1. Trim analysis merely confirms this result with a descent gradient of -9.3% just after takeoff!

We now have hazard severity assigned for failures of all the different components given in Fig. 6. The corresponding failure rate requirements for the X-57 can be obtained from Assessment Level II ($\leq$ 1 pax., multi-engine) in Table 1. The next section will look at determining component failure rates using a Bayesian probability approach and utilizing the loss function for compliance assessment.

B. Bayesian Probability Estimation

The probability distribution of component failures is evaluated using a Bayesian approach. For all components in Fig. 6, a Poisson likelihood model is assumed since failures generally occur during operation with the number of failures and corresponding operating time being the information documented [35]. A prior is selected based on an analyst's subjective bias about the component failure rate. In the present work, an initial Jeffry's non-informative conjugate prior is assumed which is updated using weighted historical data to generate an analyst's prior. For Poisson likelihood models, a Jeffry's non-informative conjugate prior is a Gamma distribution with shape $\alpha = 0.5$, and rate $\beta = 0$. Since a Gamma prior is conjugate to the Poisson likelihood, the posterior also takes the form of a Gamma distribution [35]. In a gamma distribution used for failure analysis, the shape parameter α can be interpreted as the number of failures, while the rate parameter β can be interpreted as the number of hours of operational experience with a component. Thus, high value of β can be interpreted as having a lot of operating hours experience, while lower value indicates a lack of experience and is likely to result in a much wider spread in the posterior distribution. Similarly, higher α values for a given rate parameter means a component is likely to have higher failure rates. Recent data sources are used next to update the analyst's prior to get a component's failure rate posterior. In sources where point values are provided for failure rates, Dezfuli et al. [35] provide a method to convert these to likelihood estimates, which are then used here to reach a posterior distribution.

1. Battery Posterior

An analyst's prior is constructed by updating a non-informative prior with historical data [52, 53] weighted at just 10% applicability since a lot of the historical data is not for Li-ion batteries.

$$Non-informative\ Prior \quad : \quad \lambda_{prior} \sim Gamma(\alpha = 0.5, \beta = 0) \tag{6}$$

$$Likelihood \quad : \quad y_i|\lambda \sim Poisson(\lambda t_i, y_i) \propto \frac{(\lambda t_i)^{y_i} e^{-\lambda t_i}}{y_i!} \tag{7}$$

$$\begin{aligned} Analyst\ Prior \quad &: \quad \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 0.5 + \Sigma y_i, \beta = 0 + \Sigma t_i) \\ &: \quad \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 11.45, \beta = 3966800) \end{aligned} \tag{8}$$

Eq. 12 can now be used as an analyst's prior. Data available for lithium ion batteries includes a recent NASA report [54] that suggested using 9.3 failures per million hours. Additionally, Boeing 787 reported two battery safety events in about 104000 combined flight hours of battery operation (2 batteries per aircraft, 52000 flight hours) [55], while NPRD-2016 [56] provides 8 failures in 2.6735E5 hours of operation for battery packs. This results in the following battery failure rate posterior:

$$Analyst\ Prior \quad : \quad \lambda_{prior_A} \sim Gamma(\alpha = 11.45, \beta = 3966800) \tag{9}$$

$$Likelihood \quad : \quad y_i|\lambda \sim Poisson(\lambda t_i, y_i) \tag{10}$$

$$Posterior \quad : \quad \lambda_{posterior}|\bar{y} \sim Gamma(\alpha = 30.75, \beta = 5338150) \tag{11}$$

2. Electric Motor Posterior

Similar to a battery, an analyst's prior is constructed by updating a non-informative prior with historical data [52, 53, 57] with a 10% weighting since it includes data for old electric motors.

$$Analyst\ Prior \ : \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 26.15, \beta = 1.2417E7) \tag{12}$$

Ref. [54] suggests using 9.24 failures per one million hours. Ref. [58] provides a failure rate of 6.6E-5 per flight hour for three-phase electric drives(applied with a weight of 10x), while NPRD [56] provides additional failure rates of 7.23887E-5 and 3.9586E-5 per hour. The posterior is given by:

$$Posterior \ : \lambda_{posterior}|\bar{y} \sim Gamma(\alpha = 41.39, \beta = 15446550) \tag{13}$$

3. Motor Inverter Posterior

An analyst's prior is constructed by updating a non-informative prior with historical data [52] weighted 10% as before.

$$Analyst\ Prior \ : \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 4.5, \beta = 286940.5) \tag{14}$$

Ref. [54] suggests using 4.75 failures per million hours. Ref. [58] provides a failure rate of 1.5E-4 per flight hour (applied with a weight of 10x) for electronics related to three-phase electric drives. The final posterior is:

$$Posterior \ : \lambda_{posterior}|\bar{y} \sim Gamma(\alpha = 14.25, \beta = 1345800) \tag{15}$$

4. Traction Power Bus Posterior

An analyst's prior is constructed by updating a non-informative prior with historical data [52, 53] weighted 10% as before.

$$Analyst\ Prior \ : \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 0.85, \beta = 8,467,600) \tag{16}$$

Note that this prior suggests that the analyst believes an electric bus is likely to fail less than once in over 8 million hours! NPRD [56] data includes zero failures for 1363267 hours of operating experience for electric buses. Together, the posterior is:

$$Posterior \ : \lambda_{posterior}|\bar{y} \sim Gamma(\alpha = 0.85, \beta = 9830867) \tag{17}$$

5. Pre-Charger Posterior

Failure data for a pre-charger was not found readily available in literature by the authors. However, upon closer inspection (as a Bayesian analyst may have to do to determine the prior), a pre-charger typically incorporates a resistor and a contactor to manage a sudden rush of current from damaging the inverter circuit. An analyst's prior is therefore constructed by updating a non-informative prior with historical data for the two components taken in series [53, 57] weighted 20% for the connector switches, and 100% for the resistor.

$$Analyst\ Prior \ : \lambda_{prior_A}|\bar{y} \sim Gamma(\alpha = 5.62, \beta = 1000000) \tag{18}$$

Since no data was found for pre-charger failures, the prior becomes the posterior (an enabling feature of Bayesian probability theory):

$$Posterior \ : \lambda_{posterior}|\bar{y} \sim Gamma(\alpha = 5.62, \beta = 1000000) \tag{19}$$

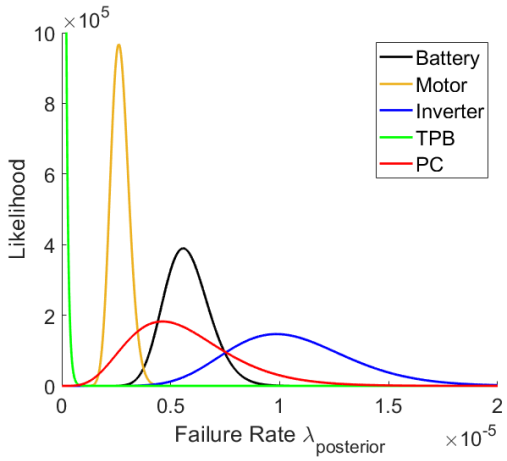


Fig. 9 Component failure rate: Bayesian posterior distributions pdf

C. Making a Compliance Assessment

Combining table 5 with table 1 for an assessment level II (≤ 1 pax, multiengine) X-57 airplane provides us with component failure rate requirements. Minor, Major, Hazardous, and Catastrophic failures must have a failure rates $\leq 10^{-3}$, $\leq 10^{-5}$, $\leq 10^{-6}$ and $\leq 10^{-7}$ per flight hour respectively. With the component level reliability (allowable failure rate) requirements now available, and failure rate posteriors available from Sec. IV.B, the Bayesian decision framework described in Sec. III.C is now utilized to determine compliance finding. Table 6 gives a simplified loss function to be used in the present work. The rational behind this loss function is as follows [14]: (i) Finding a component to be

compliant when in fact it is not can be a costly mistake and is therefore penalized the highest, (ii) Finding a component to be non-compliant when in fact it is compliant, while undesirable, is not as undesirable as the previous case, and is therefore penalized to a lesser extent, (iii) Finding a component to be (non-) compliant when it is in fact (non-) compliant is desirable, and is given a negative score to indicate a negative loss (desirable). The loss function considered here is merely an example and can be customized by decision makers as needed in order to better suit their purpose.

Table 6 Loss function $L(X, a)$

True State	**Decision Action** a	
X	$a_1 = \{Compliant\}$	$a_2 = \{Non-Compliant\}$
$X_1 = \{Compliant\}$	-2	1
$X_2 = \{Non-Compliant\}$	4	-2

The Bayesian expected loss given by Eq. 2 gets simplified because of the loss function provided by Table 6 to give,

$$\rho(a_1, p) = L(X_1, a_1) \cdot p + L(X_2, a_1) \cdot (1 - p) \quad (20)$$

$$\rho(a_2, p) = L(X_1, a_2) \cdot p + L(X_2, a_2) \cdot (1 - p) \quad (21)$$

Where $p = p(\lambda_{posterior} \leq \lambda_{req})$ is the probability of the component meeting its requirements computed using the posteriors and are given in Table 7. As stated in Sec. III.C, the minimum of the expected loss given by equations 20-21 should inform the compliance action to be taken by the analyst. Note that due to the linear nature of the expected loss function, a simple analytical simplification tells us that an action $a_1 = Compliant$ will be taken when $p \geq 0.857$, while action $a_2 = Non-Compliant$ will be taken by the analyst otherwise. However, the expected loss provided by Eq. 2 allows for great flexibility in defining the loss function to suit the analyst's needs, and is also much more intuitive in terms or penalizing or rewarding compliance decision actions that reflect the true state.

Table 7 Probability of meeting failure rate requirements

Component	**Battery-B**	**TPB-BL**	**CM-1**	**Inv-1B**	**PC-1B**	**Mot-01**	**Inv-01**	**PC-01**
$p(\lambda_{posterior} \leq \lambda_{req})$	0	0.99997	0	0.45028	0.94999	1	1	1

Table 8 Expected loss due to available decision actions

Component	**Battery-B**	**TPB-BL**	**CM-1**	**Inv-1B**	**PC-1B**	**Mot-01**	**Inv-01**	**PC-01**
$\rho(a_1, p)$	4	-1.99982	4	1.29832	-1.69994	-2	-2	-2
$\rho(a_2, p)$	-2	0.99991	-2	-0.64916	0.84997	1	1	1
Decision Action	a_2	a_1	a_2	a_2	a_1	a_1	a_1	a_1

Table 8 gives the expected loss for the decision actions a_1, a_2 for the different components of interest in the X-57 power systems architecture denoted by Fig. 6. The decision action simply minimizes the loss function, and is provided for each component. For the X-57 Mod-IV architecture of interest in the present case study, the main batteries, cruise motors, and their inverters were found to be non-compliant with the safety requirements generated. The cruise motor pre-chargers, traction power buses, and the distributed high lift propulsor system components – motors, inverters, and pre-chargers were all found compliant with the allocated reliability requirements.

V. Conclusions

A Bayesian safety assessment framework that can address some of the problems faced by traditional methods while dealing with novel architectures and technologies was proposed. To demonstrate its utility, the proposed method was implemented in a case study on the X-57 Mod.IV. Continuous functional hazard assessment was applied to the

traction power system using the maximum potential flight path angle metric to generate hazard severity curves as a function of power (thrust) degradation scenarios. A network approach to bottom-up failure analysis provided the effect of component failures on the system function of interest (Generate Power). Combining the two resulted in allocation of reliability requirements directly to the component level. To take it one step further, a preliminary 6-DoF model of the X-57 was created using the in-house DELPHI framework to perform trimmability analysis on the different unique off-nominal scenarios. These identified battery failure as a catastrophic scenario, with loss of cruise motor or the traction power buses as the next most critical (Hazardous). Bayesian failure rate posteriors were computed using a mix of vintage data to generate priors, and recently available data to inform the likelihood. Finally, a Bayesian decision theoretic framework was utilized to determine compliance finding of the different components of the X-57 traction power system. While most components were found to be compliant with failure rate requirements, the main batteries, cruise motors, and cruise motor-inverters were found to be non-compliant in the process.

It is important to pause here and acknowledge the numerous places where choices made by the authors can impact the results presented above. The use of AVL for computing lateral aerodynamic and control derivatives, while enabling for early design stages, is likely to introduce error into the results of trim solutions under off-nominal situations. It is used here as a good first guess at these parameters in early preliminary design. Similarly, the sensitivity of the results to numerous other modeling assumptions can be considered in the future. The component failure rate posteriors generated using Bayesian probability theory are by definition, subjective. Subject matter experts (SMEs) may come up with different posterior distributions – in fact, that is the intent and enabling feature of a Bayesian approach. Finally, the simplified loss function used in the present work seeks to demonstrate the value of utilizing a Bayesian decision theoretic framework for compliance finding. Once again, SMEs are free to define their own loss functions for compliance assessment. The idea of the present work is to demonstrate the value of the proposed approach in enabling a physics-based and mathematically robust approach to safety risk assessment of novel concepts, architectures, and technologies. Analysts may use the proposed framework with their own performance analysis tools, failure rate posteriors, and loss functions to evaluate such architectures.

Appendix

A. Simulation Environment

The flight dynamics simulation environment used in this work is the Dynamic Environment for Loads Prediction and Handling Investigation (DELPHI) [59–61] framework developed at the Aerospace Systems Design Lab. DELPHI is developed as an object-oriented python code which can accept any aircraft model, any desired maneuver, and simulate the flight dynamics. A high-level view of DELPHI is shown in Fig. 10.

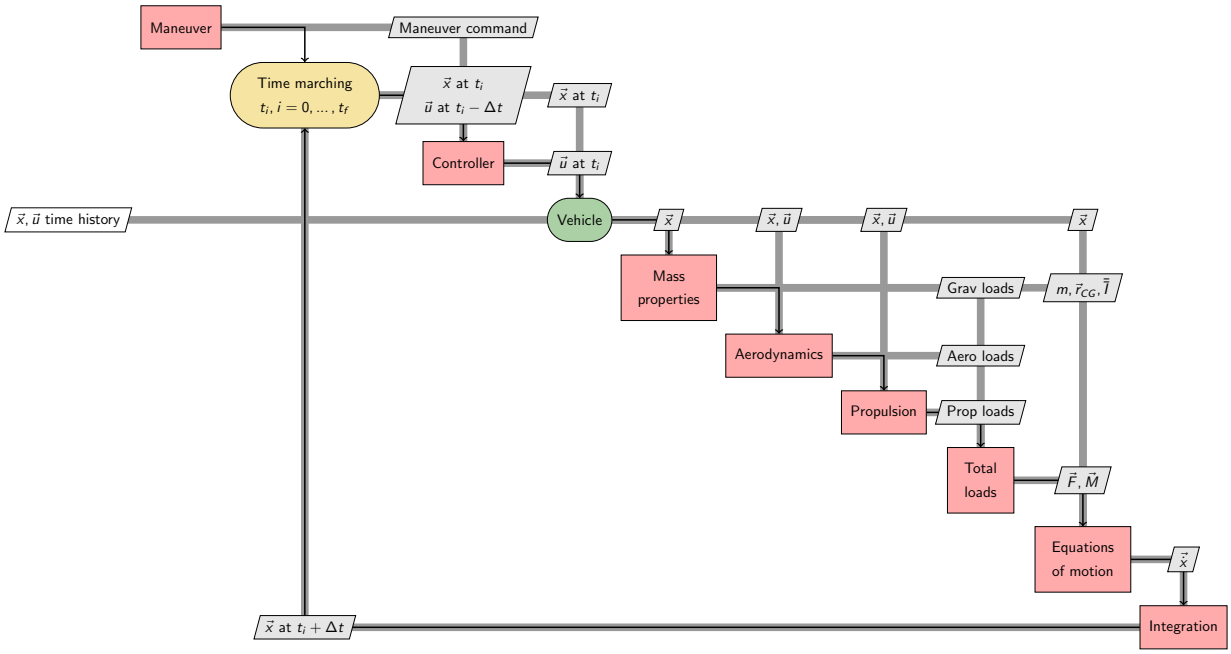


Fig. 10 DELPHI framework

A desired maneuver can be specified in the *Maneuver block*. The *Controller block* compares the desired maneuver to the current state of the aircraft and produces a control vector $\vec{u}$. The control vector specifies all control surface deflection and throttle settings on the vehicle. The *Vehicle block* contains within it the mass properties, aerodynamics and propulsion. Given the current state vector, $\vec{x}$, and control vector $\vec{u}$, the vehicle block calls appropriates methods to compute the loads due to gravity, aerodynamics and propulsion. The net loads, $\vec{F}\&\vec{M}$, are sent to the *Equations of Motion block* which computes the time derivative of the states vector, $\dot{\vec{x}}$. $\dot{\vec{x}}$ is integrated forward in time using an appropriate time-integration scheme to obtain the states vector at the next time step, $\vec{x}$ at $t_i + \Delta t$. The entire loop is time-marched till the final time t_f is reached.

The *Vehicle block* is implemented such as to allow the user to provide an arbitrary number of aircraft control surfaces and propulsion devices. Flexibility is offered to allow the data for propulsion and aerodynamics to come on any source- be it simple look-up tables, or function calls to an analysis code.

The equations of motion are cast about a fixed reference point O rather than the CG. This enables, for instance, the dynamics of a moving CG (e.g., due to decreasing fuel mass or fuel transfer) to be modeled. The force and moment equations in vector form are given below:

$$\vec{F}_{total} = m\left(\dot{\vec{V}}_0 + \vec{\omega}\times\vec{V}_0 + \ddot{\vec{r}}_g + \dot{\vec{\omega}}\times\vec{r}_g + 2\,\vec{\omega}\times\dot{\vec{r}}_g + \vec{\omega}\times(\vec{\omega}\times\vec{r}_g)\right), \tag{22}$$

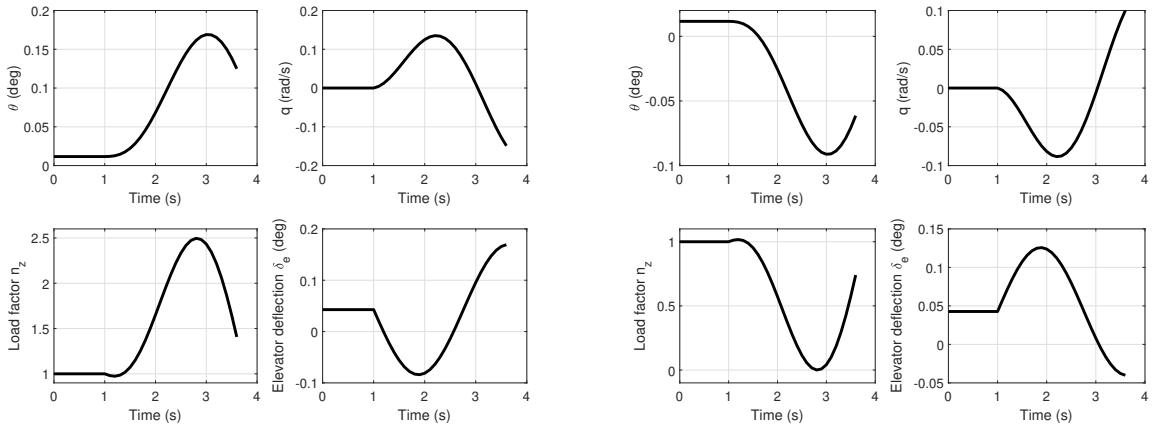
$$\vec{M}_{total} = \bar{\bar{I}}\dot{\vec{\omega}} + \vec{\omega}\times\bar{\bar{I}}\omega + m\,\vec{r}_g\times\left(\dot{\vec{V}}_0 + \vec{\omega}\times\vec{V}_0\right), \tag{23}$$

where $\vec{r}_g$ is the position vector running from O to the center of gravity (CG) of the aircraft, $\vec{V}_0 = \{u, v, w\}^T$ the velocity of the reference point O, $\vec{\omega} = \{p, q, r\}^T$ the angular velocity of the aircraft, and $\bar{\bar{I}}$ the mass moment of inertia matrix of

the aircraft about O. The more specific case where the reference point O coincides with the CG can be obtained by setting $\vec{r}_g = 0$ in the above. Kinematic relationships are used to obtain the derivatives of the Euler angles ϕ, θ, and ψ from the angular rates p, q, and r, and also derivatives of the position x_0, y_0, and z_0 of the reference point O from the velocities u, v, and w. The resulting system of 12 nonlinear ordinary differential equations (in $u, v, w, p, q, r, \phi, \theta, \psi, x_0, y_0, z_0$) for six degrees-of-freedom rigid body motion is numerically integrated to obtain the motion history of the aircraft during the maneuver.

The environment has been validated by simulating 14 CFR Part 25- Subpart C specified maneuvers: the checked-pitch maneuver, the rudder-kick maneuver, and the rolling maneuver for a representative business jet aircraft [59, 61]. Consider the checked-pitch maneuver. Sample results for flight condition $h = 9144$m and $M = 0.75$ are shown below. Fig. 11a shows the 2.5g pull-up maneuver, and Fig. 11b shows the 0g push-down maneuver.

As seen in Fig. 11a, the maneuver starts at 1g trim condition. The trim elevator deflection is seen. After 1 second, the maneuver is initiated by deflecting the elevator up (negative) to lower the lift produced, and hence pitch the aircraft up. The deflection is such that the load factor reaches 2.5. The 0g push-down maneuver has a similar behavior, but with the elevator deflected down (positive) to pitch the aircraft down.



(a) 2.5g pull-up maneuver **(b) 0g push-down maneuver**

Fig. 11 Checked-pitch maneuver

B. X-57 Aircraft Model

An X-57 aircraft model consisting of geometric data, mass properties, propulsion, and aerodynamics was built using open-source data available. The subsequent sections describe these individually.

1. Geometry

Geometric details of the X-57 are obtained from the publicly available OpenVSP model provided by NASA [62]. Tables 9, 10, and 11 give the geometric details of the wing, stabilator, and vertical tail respectively.

2. Mass Properties

The mass properties of the X57 are built-up from component mass properties. Each cruise motor is assumed to have a mass of 117 lbs, while each high-lift motor is assumed to have a mass of 15 lbs [63]. The locations of the motors are obtained from the OpenVSP model and are given in Table 14. The battery is assumed to be located at the wing quarter chord and to have a mass of 860 lbs [63]. Procedures and equations provided in Ref. [64] are utilized for computing inertia properties of the wing, empennage, and the fuselage. The component mass build-up is given in Table 12, and the net aircraft mass properties are given in Table. 13.

Table 9 X57 wing geometric specifications

Parameter	Value	Unit
Planform area- S_{wing}	9600.048	in^2
Wingspan- b_{wing}	379.56	in
Reference chord- c_{wing}	25.56	in
Aspect ratio- AR_{wing}	15	
Incidence angle	2	deg

Table 10 X57 vertical tail geometric specifications

Parameter	Value	Unit
Planform area- S_{vt}	3021.28	in^2
Span- b_{vt}	63.82	in
Reference chord- c_{vt}	56.69	in
Leading edge sweep	37.45	deg

Table 11 X57 stabilator geometric specifications

Parameter	Value	Unit
Planform area- S_{stab}	3793.73	in^2
Span- b_{stab}	123.81	in
Reference chord- c_{stab}	30.64	in

3. Propulsion

The engine locations relative to the CG (and the flight dynamics reference point about which the EoMs are cast) is given in Table 14. There are two types of motors:

1) Cruise motors at the wingtip
2) Six high-lift motors distributed along each side of the wing

The wingtip motors are controlled by changing the throttle τ. The throttle setting changes the RPM of the motors linear from minimum value of 0 to a maximum value of 2500. The RPM ω is given by:

$$\omega = \omega_{min} + \tau(\omega_{max} - \omega_{min}) \tag{24}$$

The diameter of the propeller d is 4 feet, and the thrust coefficient is 3.77×10^{-8}. The thrust produced by the motors is given by:

$$T_{wingtip} = C_T \rho \omega^2 d^4 \tag{25}$$

where ρ is the density of the air. The dependence of the thrust on the altitude at which the aircraft is flying is taken into account through the density. It is assumed that there is no dependence of Mach number on C_T.

The high-lift motors are not controlled by throttle. They are either on or off. When on, the thrust they produce depends on the equivalent airspeed of the aircraft as given in Table 15. Above 93 KEAS, they do not produce any thrust.

4. Aerodynamic Build-Up for the X-57

The aerodynamics is broken into two parts- longitudinal, and lateral aerodynamics. The basis of the longitudinal aerodynamic model for this work are regressions which provide aerodynamic coefficients in the wind frame. The regressions are obtained by digitizing the data in Deere et al. [46] and fitting polynomial linear regressions through the data. A component build-up approach is used where the aerodynamic coefficients of the entire aircraft is found by adding contributions of each component- wings, nacelles, pylons, stabilator, fuselage, and vertical tail. The aerodynamic coefficients must be a function of the following:

- States
  - Angle of attack: α
  - Sideslip angle: β
  - Angular rates: p, q, r

Table 12 Mass build-up of X57 aircraft

Parameter	Value	Unit
2 × cruise motor	106.14	kg
12 × cruise motor	81.65	kg
Battery	390.08	kg
Empennage	27.3	kg
Fuselage	235.87	kg
Landing gear	61.15	kg
Wing	152.88	kg
2 × pilot	170	kg
Misc	135.7	kg
Total	1360.77	kg

Table 13 Mass properties of X57 aircraft

Parameter	Value	Unit
Weight	1360.77	kg
I_{xx}	4314.08	$kg.m^2$
I_{xy}	-232.85	$kg.m^2$
I_{xz}	-2563.29	$kg.m^2$
I_{yy}	18656.93	$kg.m^2$
I_{yz}	-62.42	$kg.m^2$
I_{zz}	22340.21	$kg.m^2$

Table 14 X57 right engines locations relative to CG. The values are given in the flight dynamics body-fixed reference frame (x-forward, y-right, z-down). All values are in inches

Engine	x offset	y offset	z offset
Wingtip propulsor	13.01	189.74	-0.958
Distributed propulsor 1	15.39	34.98	4.2
Distributed propulsor 2	13.41	57.66	4.2
Distributed propulsor 3	15.39	80.34	4.2
Distributed propulsor 4	11.92	103.02	4.2
Distributed propulsor 5	13.90	125.7	4.2
Distributed propulsor 6	10.41	148.38	4.2

- Controls
  - Stabilator incidence angle: δ_s
  - Trim-tab deflection angle: δ_{tt}
  - Flap deflection angle: δ_f
  - Aileron deflection angle: δ_a
  - Rudder deflection angle: δ_r
  - High lift propeller blowing (boolean)

The lift coefficient is found as:

$$C_L(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{L_{\text{blower}}} \frac{\#\text{ of blowers } ON}{12} + C_{L_{\text{wing + tip-nacelle}}} + C_{L_{\text{flap}}} + C_{L_{\text{HLN}}} + C_{L_{\text{fuse+Vtail}}} + C_{L_{\text{stab}}} \frac{S_{stab}}{S_{wing}} \tag{26}$$

Note: it is assumed that the lift coefficient is not affected by the sideslip angle. The drag coefficient is similarly found as:

$$C_D(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{D_{\text{blower}}} \frac{\#\text{ of blowers } ON}{12} + C_{D_{\text{wing + tip-nacelle}}} + C_{D_{\text{flap}}} + C_{D_{\text{HLN}}} + C_{D_{\text{fuse+Vtail}}} + C_{D_{\text{stab}}} \frac{S_{stab}}{S_{wing}} \tag{27}$$

The moment coefficient is found as:

$$C_m(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{m_{\text{blower}}} \frac{\#\text{ of blowers } ON}{12} + C_{m_{\text{wing + tip-nacelle}}} + C_{m_{\text{flap}}} + C_{m_{\text{HLN}}} + C_{m_{\text{fuse+Vtail}}} + C_{m_{\text{stab}}} \frac{S_{stab} c_{stab}}{S_{wing} c_{wing}} \tag{28}$$

Table 15 High-lift motors thrust dependence on V_{EAS}

Velocity (KEAS)	0	17	24	31	38	58	64	70	76	84	93
Thrust (lbf)	0	10	20	30	40	50	40	30	20	10	0

Table 16 Estimated lateral aerodynamic coefficients of the X57

	β	p	r	δ_a	δ_r
C_Y	-1.4487	-0.0883	0.2772	0.0026	0.181
C_n	0.2678	0.0321	-0.257	0.0039	-0.1408
C_l	-0.0131	-0.6742	0.0569	0.2149	0.0143

To the best of the authors' knowledge there is no publicly available lateral aerodynamic data for the X57. The Vortex Lattice Method (VLM) is low-fidelity method for the pressure field approximation using linearized potential flow. In the VLM, the lifting surfaces are model as discretized vortex panels following Biot-Savart Law and Kutta-Joukwski Theory, while the non-lifting bodies are model as sources/sinks or doublets to enforce the non-penetrating condition. Due to its nature of linearization, the VLM is able to quickly compute the stability and control derivatives. An open-source vortex lattice method software, AVL [65], is used to obtain the lateral aerodynamic coefficients. The authors acknowledge the limitations posed by a linearized estimation method while ignoring the effects of swirl and sidewash generated by multiple high-lift and wingtip propellers. However, the intent of the present work is to generate a quick estimate by utilizing data available in early-preliminary design stages. For that reason, the results generated were found adequate for the purpose of the present research. The lateral aerodynamic coefficients from AVL are given in Table 16. The net lateral coefficients are found as:

$$C_Y = C_{Y_\beta}\beta + C_{Y_p}\hat{p} + C_{Y_r}\hat{r} + C_{Y_{\delta_a}}\delta_a + C_{Y_{\delta_e}}\delta_e + C_{Y_{\delta_r}}\delta_r \tag{29}$$

$$C_l = C_{l_\beta}\beta + C_{l_p}\hat{p} + C_{l_r}\hat{r} + C_{l_{\delta_a}}\delta_a + C_{l_{\delta_e}}\delta_e + C_{l_{\delta_r}}\delta_r \tag{30}$$

$$C_n = C_{n_\beta}\beta + C_{n_p}\hat{p} + C_{n_r}\hat{r} + C_{n_{\delta_a}}\delta_a + C_{n_{\delta_e}}\delta_e + C_{n_{\delta_r}}\delta_r \tag{31}$$

where

$$\hat{p} = \frac{pb}{2V} \tag{32}$$

$$\hat{r} = \frac{rb}{2V} \tag{33}$$

Finally, the aerodynamic loads are computed from the coefficients as:

$$L = \bar{q}S_W C_L \tag{34}$$

$$D = \bar{q}S_W C_D \tag{35}$$

$$Y = \bar{q}S_W C_Y \tag{36}$$

$$l = \bar{q}S_W bC_l \tag{37}$$

$$m = \bar{q}S_W cC_m \tag{38}$$

$$n = \bar{q}S_W bC_n \tag{39}$$

The above loads are obtained in the wind-axis and are rotated to the body-fixed axis frame before being used in the equations of motion.

C. A Network Approach to Bottom-Up Failure Analysis

For a given system represented as a network of prime movers (nodes A_B), terminal components that satisfy system function (A_T) and intermediate components, Algorithm 1 explains how system failures states can be obtained if any

component (A_i) fails:

Algorithm 1: Generate a set of terminal components that fail if any system component fails

Result: Set of A_T that fail if component A_i fails
Generate system adjacency matrix M;
Set $F = M$;
Set $F(i,:) = 0$ % set out-going network connections to 0;
Initialize C = zeros(size(M));
Initialize jj = 1;
while F^{jj} *is not zero* **do**
    C = C + F^{jj};
    jj = jj+1;
end
truncate C to keep rows corresponding to all A_B and columns corresponding to all A_T and assign to T;
Initialize kk = 1;
while $kk \leq$ *numCols in T* **do**
    if *max(T(:,kk)) == 0* **then**
        A_T corresponding to kk^{th} column of T has failed;
        Store A_T;
        kk = kk+1;
    else
        A_T corresponding to kk^{th} column of T has NOT failed;
    end
end

References

[1] FAA, "Revision of Airworthiness Standards for Normal, Utility, Acrobatic, and Commuter Category Airplanes," Federal Register, online: https://www.govinfo.gov/content/pkg/FR-2016-12-30/pdf/2016-30246.pdf, 2017.

[2] "SAE ARP4761: Guidelines and Methods for conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," Standard, SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-001, 1996.

[3] "SAE ARP4754: Guidelines for Development of Civil Aircraft and Systems," Standard, SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-001, 2010.

[4] Moir, I., Seabridge, A., and Jukes, M., *System Safety*, chapter and pages, pp. 119–158. URL http://ebookcentral.proquest.com/lib/gatech/detail.action?docID=1469444.

[5] Hasson, J., and Crotty, D., "Boeing's safety assessment processes for commercial airplane designs," *16th DASC. AIAA/IEEE Digital Avionics Systems Conference. Reflections to the Future. Proceedings*, Vol. 1, IEEE, 1997, pp. 4.4–1 – 4.4–7.

[6] Ericson, C. A., *Hazard Analysis Techniques for System Safety*, Wiley-Interscience, Hoboken, N.J., 2005.

[7] Saglimbene, M. S., "Reliability analysis techniques: How they relate to aircraft certification," *Annual Reliability and Maintainability Symposium*, IEEE, 2009, pp. 218–222.

[8] Caldwell, R. E., and Merdgen, D. B., "Zonal analysis: the final step in system safety assessment (of aircraft)," *Annual Reliability and Maintainability Symposium*, IEEE, 1991, pp. 277–279.

[9] Bleu-Laine, M.-H., Bendarkar, M. V., Xie, J., Briceno, S., and Mavris, D. N., "A Model-Based System Engineering Approach to Normal Category Airplane Airworthiness Certification," *AIAA Aviation Forum*, Dallas, TX, 2019.

[10] Bendarkar, M. V., Xie, J., Briceno, S., Harrison, E. D., and Mavris, D. N., "A Model-Based Aircraft Certification Framework for Normal Category Airplanes," *AIAA Aviation Forum*, VIRTUAL EVENT, 2020. https://doi.org/https://doi.org/10.2514/6.2020-3096.

[11] Washington, A., Clothier, R. A., and Williams, B. P., "A Bayesian approach to system safety assessment and compliance assessment for Unmanned Aircraft Systems," *Journal of Air Transport Management*, Vol. 62, 2017, pp. 18 – 33. https://doi.org/10.1016/j.jairtraman.2017.02.003.

[12] "ASTM F3230-17: Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft," Standard, ASTM, West Conshohocken, PA, United States, 2017.

[13] Armstrong, M., "Identification Of Emergent Off-nominal Operational Requirements During Conceptual Architecting Of The More Electric Aircraft," Ph.D. thesis, Georgia Institute of Technology, 2011.

[14] Bendarkar, M. V., Behere, A., Briceno, S. I., and Mavris, D. N., "A Bayesian Safety Assessment Methodology for Novel Aircraft Architectures and Technologies using Continuous FHA," *AIAA Aviation 2019 Forum*, 2019, p. 3123. https://doi.org/10.2514/6.2019-3123.

[15] Kaplan, S., and Garrick, B. J., "On the quantitative definition of risk," *Risk analysis*, Vol. 1, No. 1, 1981, pp. 11–27.

[16] Foot, P., "The Problem of Abortion and the Doctrine of the Double Effect," *Oxford Review*, Vol. 5, 1967, pp. 5–15. https://doi.org/10.5840/monist197659224.

[17] Jarvis Thomson, J., "The trolley problem," *Yale Law Journal*, Vol. 94, No. 6, 1985, p. 5.

[18] Thomson, J. J., "Killing, letting die, and the trolley problem," *The Monist*, Vol. 59, No. 2, 1976, pp. 204–217.

[19] Allenby, K., and Kelly, T., "Deriving safety requirements using scenarios," *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, IEEE, 2001, pp. 228–235.

[20] Ruijters, E., and Stoelinga, M., "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Computer Science Review*, Vol. 15-16, 2015, pp. 29–62. https://doi.org/10.1016/j.cosrev.2015.03.001.

[21] Kabir, S., "An overview of fault tree analysis and its application in model based dependability analysis," *Expert Systems with Applications*, Vol. 77, 2017, pp. 114–135.

[22] Lee, H.-J., and LEE, H.-W., "Method for assessing the electric power system reliability of multiple-engined aircraft," *Journal of Aircraft*, Vol. 30, No. 3, 1993, pp. 413–414.

[23] Hasan, S., Hemm, R., Houser, S., and Reveley, M., "Integrated Safety Benefits Analysis of NASA Aviation Safety Program Technologies," *AIAA's Aircraft Technology, Integration, and Operations (ATIO) 2002 Technical Forum*, 2002, p. 5893.

[24] Hemm, R., Horio, B., and DeCicco, A., "Assessment of system safety risks for NextGen concepts and technologies," *12th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference and 14th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, 2012, p. 5547.

[25] Papathakis, K. V., Burkhardt, P. A., Ehmann, D. W., and Sessions, A. M., "Safety Considerations for Electric, Hybrid-Electric, and Turbo-Electric Distributed Propulsion Aircraft Testbeds," *53rd AIAA/SAE/ASEE Joint Propulsion Conference*, 2017. https://doi.org/10.2514/6.2017-5032.

[26] Woodham, K. P., Graydon, P., Borer, N. K., Papathakis, K. V., Stoia, T., and Balan, C., "FUELEAP Model-Based System Safety Analysis," *2018 Aviation Technology, Integration, and Operations Conference*, 2018. https://doi.org/10.2514/6.2018-3362.

[27] Amendola, A., and Reina, G., "Event Sequences and Consequence Spectrum: A Methodology for Probabilistic Transient Analysis," *Nuclear Science and Engineering*, Vol. 77, No. 3, 1981, pp. 297–315. https://doi.org/10.13182/NSE81-A19840.

[28] Dominguez-Garcia, A. D., Kassakian, J. G., Schindall, J. E., and Zinchuk, J. J., "An integrated methodology for the dynamic performance and reliability evaluation of fault-tolerant systems," *Reliability Engineering & System Safety*, Vol. 93, No. 11, 2008, pp. 1628–1649.

[29] Borer, N., Claypool, I., Clark, D., West, J., Somervill, K., Odegard, R., and Suzuki, N., "Model-driven development of reliable avionics architectures for Lunar Surface Systems," *2010 IEEE Aerospace Conference*, IEEE, 2010, pp. 1–21.

[30] Paté-Cornell, M., "Uncertainties in risk analysis: Six levels of treatment," *Reliability Engineering System Safety*, Vol. 54, No. 2, 1996, pp. 95 – 111. https://doi.org/10.1016/S0951-8320(96)00067-1.

[31] Zaretsky, E., Hendricks, R. C., and Soditus, S., "Weibull-based design methodology for rotating aircraft engine structures," Report NASA/TM-2002-211348, NAS 1.15:211348, E-13091, NASA, June 2002.

[32] Jardine, A., Anderson, P., and Mann, D., "Application of the Weibull proportional hazards model to aircraft and marine engine failure data," *Quality and reliability engineering international*, Vol. 3, No. 2, 1987, pp. 77–82. https://doi.org/10.1002/qre.4680030204.

[33] Armstrong, M., Garcia, E., and Mavris, D., "Aircraft Mission And System Failure Considerations For Functional Induction Based Conceptual Architecture Design," 27th International Congress of Aeronautical Sciences, Nice, France, 2010.

[34] Lam, H. T., and Szeto, K. Y., "Optimization of Reliability of Network of Given Connectivity using Genetic Algorithm," *arXiv preprint arXiv:1412.4218*, 2014.

[35] Dezfuli, H., Kelly, D., Smith, C., Vedros, K., and Galyean, W., "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," Tech. Rep. NASA/SP-2009-569, National Aeronautics and Space Administration, 2009.

[36] An, D., Choi, J., and Won, J., "Integrated Bayesian reliability analysis under input variable and metamodel uncertainties," *51st AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 18th AIAA/ASME/AHS Adaptive Structures Conference 12th*, 2010, p. 2594.

[37] Banghart, M., Bian, L., Strawderman, L., and Babski-Reeves, K., "Risk assessment on the EA-6B aircraft utilizing Bayesian networks," *Quality Engineering*, Vol. 29, No. 3, 2017, pp. 499–511. https://doi.org/10.1080/08982112.2017.1319957.

[38] Bonis, A., "Bayesian Reliability Demonstration Plans," *5th Annual Reliability and Maintainability Conference*, 1966. https://doi.org/10.2514/6.1966-25112.

[39] Youn, B., and Wang, P., "Bayesian Reliability Based Design Optimization under Both Aleatory and Epistemic Uncertainties," *11th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, 2006. https://doi.org/10.2514/6.2006-6928.

[40] "Reactor safety study. An assessment of accident risks in US commercial nuclear power plants. Executive summary," Tech. rep., United States Nuclear Regulatory Commission, 1975.

[41] Guarro, S., "Risk assessment of new space launch and supply vehicles," *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 5157–5164.

[42] Guikema, S. D., and Paté-Cornell, M. E., "Bayesian analysis of launch vehicle success rates," *Journal of spacecraft and rockets*, Vol. 41, No. 1, 2004, pp. 93–102.

[43] Kelly, D. L., "Risk Analysis of the Space Shuttle: Pre-Challenger Bayeisan Prediction of Failure," Tech. rep., Idaho National Laboratory (INL), 2008.

[44] Lee, P. M., *Bayesian statistics an introduction*, 4^{th} ed., Chichester, West Sussex ; Hoboken, N.J., 2012.

[45] Clarke, S., Redifer, M., Papathakis, K., Samuel, A., and Foster, T., "X-57 power and command system design," *2017 IEEE Transportation Electrification Conference and Expo (ITEC)*, IEEE, 2017, pp. 393–400. https://doi.org/10.1109/ITEC.2017.7993303.

[46] Deere, K. A., Viken, S., Carter, M. B., Viken, J. K., Cox, D. E., Wiese, M. R., and Farr, N. L., "Computational Component Build-up for the X-57 Maxwell Distributed Electric Propulsion Aircraft," *2018 AIAA Aerospace Sciences Meeting*, 2018, p. 1275.

[47] Puranik, T., Jimenez, H., and Mavris, D., "Energy-based metrics for safety analysis of general aviation operations," *Journal of Aircraft*, Vol. 54, No. 6, 2017, pp. 2285–2297.

[48] Puranik, T. G., "A Methodology for Quantitative Data-driven Safety Assessment for General Aviation," Ph.D. thesis, Georgia Institute of Technology, 2018.

[49] Marco, A. D., Duke, E., and Berndt, J., "A General Solution to the Aircraft Trim Problem," *AIAA Modeling and Simulation Technologies Conference and Exhibit*, 2007. https://doi.org/10.2514/6.2007-6703.

[50] Schnulo, S. L., Chin, J., Falck, R. D., Gray, J. S., Papathakis, K. V., Clarke, S. C., Reid, N., and Borer, N. K., *Development of a Multi-Segment Mission Planning Tool for SCEPTOR X-57*, chapter and pages. https://doi.org/10.2514/6.2018-3738.

[51] Schnulo, S. L., Hall, D., and Chin, J., "Further Development and Validation of NASA X-57 Maxwell Mission Planning Tool for Mods III and IV," *AIAA Propulsion and Energy 2019 Forum*, 2019. https://doi.org/10.2514/6.2019-4491.

[52] *Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment*, No. 508 in TECDOC Series, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 1989. URL https://www.iaea.org/publications/763/survey-of-ranges-of-component-reliability-data-for-use-in-probabilistic-safety-assessment.

[53] *Generic Component Reliability Data for Research Reactor PSA*, No. 930 in TECDOC Series, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 1997. URL https://www.iaea.org/publications/5582/generic-component-reliability-data-for-research-reactor-psa.

[54] Darmstadt, P. R., Catanese, R., Beiderman, A., Dones, F., Chen, E., Mistry, M. P., Babie, B., Beckman, M., and Preator, R., "Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems," Tech. Rep. NASA/CR-2019-220217, National Aeronautics and Space Administration, 2019.

[55] NTSB, "Auxiliary Power Unit Battery Fire Japan Airlines Boeing 787-8, JA829J," Incident Report NTSB/AIR-14/01, National Transportation Safety Board, Jan 7, 2013 2013. URL https://www.ntsb.gov/investigations/pages/boeing_787.aspx.

[56] Mahar, D., Fields, W., and Reade, J., "Nonelectronic Parts Reliability Data (NPRD-2016)," Tech. rep., Quanterion Solutions Incorporated, 2015.

[57] "Historical Reliability Data for IEEE 3006 Standards: Power Systems Reliability," *3006HistoricalData-2012 Historical Reliability Data for IEEE 3006 Standards*, 2012, pp. 1–303. https://doi.org/10.1109/IEEESTD.2012.6745993.

[58] Cao, W., Mecrow, B. C., Atkinson, G. J., Bennett, J. W., and Atkinson, D. J., "Overview of Electric Motor Technologies Used for More Electric Aircraft (MEA)," *IEEE Transactions on Industrial Electronics*, Vol. 59, No. 9, 2012, pp. 3523–3531. https://doi.org/10.1109/TIE.2011.2165453.

[59] Goron, G., Duca, R., Sarojini, D., Shah, S., Chakraborty, I., Briceno, S. I., and Mavris, D. N., "A Simulation-Based Framework for Structural Loads Assessment during Dynamic Maneuvers," *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017, p. 3767.

[60] Duca, R., Sarojini, D., Bloemer, S., Chakraborty, I., Briceno, S. I., and Mavris, D. N., "Effects of Epistemic Uncertainty on Empennage Loads During Dynamic Maneuvers," *2018 AIAA Aerospace Sciences Meeting*, 2018, p. 0767.

[61] Sarojini, D., Duca, R., Solano, H. D., Chakraborty, I., Briceno, S. I., and Mavris, D. N., "Framework to Assess Effects of Structural Flexibility on Dynamic Loads Developed in Maneuvering Aircraft," *2018 Aviation Technology, Integration, and Operations Conference*, 2018, p. 4147.

[62] NASA-LaRC, "X-57 Maxwell Simplified CRM v.4.4.1," retrieved June 8, 2020, online: http://hangar.openvsp.org/vspfiles/408, 2013.

[63] NASA, "X-57 Mini-Poster," retrieved November 16, 2020, online: https://www.nasa.gov/sites/default/files/atoms/files/x-57-litho-print-v4.pdf, 2020.

[64] Lanham, C., "Inertia Calculation Procedure for Preliminary Design," Tech. rep., AERONAUTICAL SYSTEMS DIV WRIGHT-PATTERSON AFB OH, 1979.

[65] Drela, M., and Youngren, H., *AVL 3.36 User Primer*, MIT, Feb. 2017.